

**Об утверждении Правил проведения аудита информационных систем**

***Утративший силу***

Приказ Председателя Агентства Республики Казахстан по информатизации и связи от 31 июля 2007 года № 311-п. Зарегистрирован в Министерстве юстиции Республики Казахстан 13 сентября 2007 года № 4928. Утратил силу приказом Министра связи и информации Республики Казахстан от 20 августа 2010 года № 200

      Сноска. Утратил силу приказом Министра связи и информации РК от 20.08.2010 № 200 (вводится в действие по истечении десяти календарных дней после дня его первого официального опубликования).

      В соответствии со статьей 6 Закона Республики Казахстан от 11 января 2007 года "Об информатизации" **ПРИКАЗЫВАЮ** :

      1. Утвердить прилагаемые Правила проведения аудита информационных систем.

      2. Департаменту информатизации Агентства Республики Казахстан по информатизации и связи (далее - Агентство) (Жайлаубаева А.С.) обеспечить в установленном порядке государственную регистрацию настоящего приказа в Министерстве юстиции Республики Казахстан (далее - государственная регистрация).

      3. Департаменту финансово-экономического анализа и административной работы Агентства (Уразалиев Н.Б.) после государственной регистрации настоящего приказа, в установленном порядке, обеспечить его официальное опубликование в средствах массовой информации.

      4. Контроль за исполнением настоящего приказа возложить на заместителя Председателя Агентства по информатизации и связи Дурмагамбетова Е.Д.

      5. Настоящий приказ вводится в действие по истечении десяти календарных дней после дня его первого официального опубликования.

*Председатель*

Утверждены                 
Приказом Председателя Агентства    
Республики Казахстан           
по информатизации и связи        
от 31 июля 2007 года N 311-п

**Правила проведения аудита информационных систем 1. Общие положения**

      1. Настоящие Правила проведения аудита информационных систем (далее - Правила) разработаны в соответствии с Законом Республики Казахстан от 11 января 2007 года "Об информатизации".   
      Правила определяют порядок проведения аудита информационных систем и выдачи аудиторского заключения.

      2. Аудит информационных систем осуществляется с целью:   
      оценки текущего состояния информационной системы, действий и событий, происходящих в ней;   
      установления уровня их соответствия определенным критериям, техническим регламентам, стандартам, нормативно-технической документации и (или) требованиям заказчика;   
      обеспечения эффективного и результативного функционирования информационных систем;   
      выдачи заключений по развитию и сопровождению информационных систем на основании результатов аудиторской проверки.

      3. Проведение аудита осуществляется лицом (далее - аудитором), имеющего право на проведение аудиторской деятельности, обладающего специальными знаниями и опытом работы в сфере информационных технологий, в порядке установленным уполномоченным органом в сфере информатизации.

      4. Расходы по проведению аудита информационных систем оплачивают собственники и (или) владельцы информационных систем, выступающие инициаторами проведения аудита.

**2. Основные положения аудита**

      5. Аудит может быть проведен на этапе создания, внедрения и эксплуатации информационных систем (далее - ИС).

      6. Аудит представляет собой поэтапную оценку ИС посредством определения соответствия ресурсов организации, включающих в себя технологии, приложения и оборудование, следующим критериям качества и характеристикам:   
      эффективность (уместность и соответствие поставленным задачам);   
      продуктивность (уровень выполнения поставленных задач);   
      целостность (точность и законченность информации);   
      пригодность (доступность информации требуемым бизнес - процессам, защита необходимых и сопутствующих ресурсов);   
      согласованность (исполнение нормативных и правовых документов, договоров, влияющих на бизнес-процесс);   
      надежность (уровень достоверности и правдивости информации, обеспечение бесперебойной работы ИС во время эксплуатации).

      7. Оценка соответствия критериям качества и характеристикам ИС проводится на основании предоставленной заявителем документированной информации согласно стандартам на разработку программного обеспечения и системной документации в объеме, предусмотренным договором между разработчиком и заказчиком ИС.   
      По согласованию с заявителем для аудита может использоваться дополнительная документированная информация по эксплуатации ИС, в том числе наличие сертификатов соответствия по требованиям информационной безопасности на элементы ИС, включая средства защиты электронных информационных ресурсов и информационных систем, предписаний на эксплуатацию, результаты анализа работы ИС и статистика разрешения инцендентов, регламенты, описи и спецификация оборудования, результаты хронометрических и иных измерений и т.п.   
      Управление и контроль оценки соответствия критериям качества проводится на основании контрольных результатов функционирования ИС.

      8. По результатам аудита составляется аудиторское заключение ( приложение 2 ) на соответствие критериям качества и характеристикам согласно пункта 6 Правил.

      9. Аудиторское заключение составляется не менее чем в двух экземплярах, один из которых передается заявителю, ИС которого проходила аудит, второй остается у лица, проводившего аудит.

      10. В случае внесения заявителем изменений в информационную систему, прошедшую аудит, заявитель в течение 30 календарных дней с момента начала действия внесенных изменений обращается в организацию, проводившую аудит ИС, для проведения повторного аудита или привлечь для выполнения этих работ другого аудитора.

      11. В случае если аудиторское заключение содержит отрицательные результаты по каким-либо критериям, заявитель в согласованный с рабочей группой срок может исправить недостатки, после чего пройти аудит повторно.

**3. Проведение аудита**

      12. Проведение аудита проводится на основании заявления собственника и (или) владельца ИС ( Приложение 1 ).

      13. Аудит проводится в соответствии с договором между аудитором и владельцем ИС.

      14. На основании документированной информации, представленной собственником и (или) владельцем ИС согласно пункту 7 Правил, аудитор проводит аудит в следующем порядке:   
      изучает описание ИС;   
      проверяет опытным путем соответствие ИС критериям качества и характеристикам, согласно пункту 6 Правил;   
      запрашивает у заявителя, в случае необходимости, дополнительные данные о функционировании ИС. Срок ответа на запрос рабочей группы не должен превышать 5 календарных дней;   
      готовит аудиторское заключение, которое заверяется его подписью и подписью заявителя, скрепляется оттиском печати аудитора и передается по назначению, согласно пункта 9 Правил.

      15. Срок составления аудиторского заключения определяется договором между аудитором и владельцем ИС.

      16. Аудиторское заключение носит рекомендательный характер и может:   
      учитываться собственником и (или) владельцем ИС при принятии решения о внесении изменений в ИС;   
      служить основанием для принятия решений по развитию ИС;   
      рассматриваться в судах для решения споров между заказчиками, разработчиками, другими участниками процессов создания и эксплуатации информационных систем.

      17. Аудиторское заключение имеет силу в течение всего срока действия ИС при условии, что заявитель не вносит существенных изменений в ИС, влияющих на принципы работы и характеристики, которые она имела на момент проведения аудита.

Приложение 1            
к Правилам проведения       
аудита информационных систем

**Заявление**

      Прошу провести аудит информационной системы   
\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_   
              ( *наименование информационной системы* )

владельцем которой является   
\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_   
             ( *полное название организации - Заявителя* )   
\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_   
          ( *Ф.И.О. руководителя организации - Заявителя* )   
\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_   
                 ( *адрес организации - Заявителя* )

      С Правилами проведения аудита информационных систем ознакомлен.   
Достоверность представленной информации гарантирую.

К заявлению прилагаются:   
1.\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_   
2.\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_   
3.\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_   
4.\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

                                              "\_\_\_\_" \_\_\_\_\_\_\_ 200\_\_ г.

     МП                                        Подпись \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

Приложение 2              
к Правилам проведения         
аудита информационных систем

"Утверждаю"                      
\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_          
      должность                  
\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_          
        ФИО                     
"\_\_\_\_\_\_"\_\_\_\_\_\_\_\_\_\_\_\_ \_\_\_\_\_ г.

**Аудиторское заключение**   
**по результатам проведения аудита**   
**информационной системы**

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_   
               ( *наименование информационной системы* )   
\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_   
               ( *наименование организации - Заявителя* )

на "\_\_\_\_\_"\_\_\_\_\_\_\_\_\_\_\_200\_ г.

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_   
         ( *наименование лица, осуществляющего аудит ИС* )

согласно заявления от "\_\_\_\_\_\_"\_\_\_\_\_\_\_\_\_\_\_\_200\_ г. проведен аудит в   
соответствии с Правилами проведения аудита информационных систем.

      В ходе аудиторской проверки было установлено, что данная инфор-   
мационная система удовлетворяет / не удовлетворяет ниже перечисленным   
критериям качества и характеристикам:   
1. \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_   
2. \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_   
3. \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_   
4. \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_   
5. \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

      Рекомендации по сопровождению и развитию информационной системы   
\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_   
\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_   
\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_   
\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

      Согласовано:              \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_     \_\_\_\_\_\_\_\_\_\_\_\_\_\_   
                                 ФИО заказчика           подпись

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