Об утверждении Правил проведения аттестации государственных информационных систем и негосударственных информационных систем, интегрируемых с государственными информационными системами, на соответствие их требованиям информационной безопасности и принятым на территории Республики Казахстан стандартам

Утративший силу

Постановление Правительства Республики Казахстан от 30 декабря 2009 года № 2280. Утратило силу постановлением Правительства Республики Казахстан от 23 мая 2016 года № 298

Сноска. Утратило силу постановлением Правительства РК от 23.05.2016 № 298 (вводится в действие по истечении десяти календарных дней после дня его первого официального опубликования).

В соответствии со статьей 5 Закона Республики Казахстан от 11 января 2007 года "Об информатизации" Правительство Республики Казахстан **П О С Т А Н О В Л Я Е Т** :

1. Утвердить прилагаемые Правила проведения аттестации государственных информационных систем и негосударственных информационных систем, интегрируемых с государственными информационными системами, на соответствие их требованиям информационной безопасности и принятым на территории Республики Казахстан стандартам.

2. Признать утратившим силу постановление Правительства Республики Казахстан от 17 января 2008 года № 24 "Об утверждении Правил проведения аттестации государственных информационных систем на соответствие требованиям информационной безопасности" (САПП Республики Казахстан, 2008 г., № 1, ст. 13).

3. Настоящее постановление вводится в действие со дня первого официального опубликования.

П р е м ь е р - М и н и с т р

Республики Казахстан К. Масимов

У т в е р ж д е н ы

п о с т а н о в л е н и е м Правительства

Р е с п у б л и к и К а з а х с т а н

от 30 декабря 2009 года № 2280

Правила
проведения аттестации государственных информационных систем и негосударственных информационных систем, интегрируемых с государственными информационными системами, на соответствие их требованиям информационной безопасности и принятым на территории Республики Казахстан стандартам

1. Общие положения и основные понятия

1. Настоящие Правила проведения аттестации государственных информационных систем, в том числе в соответствии с перечнем национальных электронных информационных ресурсов и национальных информационных систем, утвержденных постановлением Правительства Республики Казахстан от 1 октября 2007 года № 863, и негосударственных информационных систем, интегрируемых с государственными информационными системами, на соответствие их требованиям информационной безопасности и принятым на территории Республики Казахстан стандартам (далее - Правила) разработаны в соответствии с Законом Республики Казахстан от 11 января 2007 года "Об информатизации" и определяют порядок проведения аттестации государственных информационных систем и негосударственных информационных систем, интегрируемых с государственными информационными системами, на соответствие требованиям информационной безопасности и принятым на территории Республики Казахстан стандартам.

Настоящие Правила не распространяются на проведение аттестации государственных информационных систем, осуществляющих обработку, хранение, передачу сведений, составляющих государственные секреты, а также в защищенном исполнении (созданных и принятых в эксплуатацию в соответствии с требованиями государственного стандарта Республики Казахстан СТ РК 34.025 -2006 Защита информации. Порядок создания автоматизированных систем в защищенном исполнении. Общие положения).

Сноска. Пункт 1 в редакции постановления Правительства РК от 03.11.2011 № 1285 (вводится в действие по истечении десяти календарных дней после первого официального опубликования).

2. Основные понятия, используемые в Правилах:

1) аттестационная комиссия (далее - Комиссия) - консультативно-совещательный орган при уполномоченном органе, который рассматривает результаты аттестационного обследования и вырабатывает

соответствующие рекомендации;

2) аттестат соответствия информационной системы требованиям информационной безопасности и принятым на территории Республики Казахстан стандартам (далее - аттестат) - документ, подтверждающий факт соответствия информационной системы (далее - ИС) требованиям информационной безопасности (далее - ИБ) и принятым на территории Республики Казахстан стандартам;

3) уполномоченный орган - уполномоченный орган в сфере информатизации;

4) государственная техническая служба - республиканское государственное предприятие на праве хозяйственного ведения, созданное по решению Правительства Республики Казахстан;

5) заявитель - владелец ИС, физическое или юридическое лицо уполномоченное владельцем ИС, подавший заявку на проведение аттестации ИС на соответствие требованиям ИБ и принятым на территории Республики Казахстан стандартам.

Сноска. Пункт 2 с изменениями, внесенными постановлениями Правительства РК от 03.11.2011 № 1285 (вводится в действие по истечении десяти календарных дней после первого официального опубликования); от 28.01.2013 № 49 (вводится в действие по истечении десяти календарных дней со дня первого официального опубликования).

3. Под аттестацией ИС на соответствие требованиям ИБ и принятым на территории Республики Казахстан стандартам понимается комплекс организационно-технических мероприятий по определению фактического состояния защищенности ИС и ее соответствия требованиям ИБ и принятым на территории Республики Казахстан стандартам.

4. Эксплуатация и внедрение государственных ИС, а также всех интегрируемых с ними негосударственных ИС допускается после их аттестации на соответствие требованиям ИБ и принятым на территории Республики Казахстан стандартам.

5. Аттестация ИС на соответствие требованиям ИБ и принятым на территории Республики Казахстан стандартам осуществляется уполномоченным органом на основании аттестационного обследования ИС.

6. Аттестационное обследование ИС на соответствие требованиям ИБ и принятым на территории Республики Казахстан стандартам проводится государственной технической службой.

Сноска. Пункт 6 в редакции постановления Правительства РК от 28.01.2013 № 49 (вводится в действие по истечении десяти календарных дней со дня первого официального опубликования).

6-1. Аттестационное обследование включает:

1) проверку общей структуры на соответствие политике безопасности и размещения компонентов в структуре;

2) проверку конфигурации компонентов, являющихся составляющими ИС;

3) экспертизу организационных мер информационной безопасности эксплуатируемой ИС;

4) инструментальное обследование компонентов ИС, позволяющих пользователям получать доступ к информации в обход существующих механизмов защиты.

Сноска. Правила дополнены пунктом 6-1 в соответствии с постановлением Правительства РК от 03.11.2011 № 1285 (вводится в действие по истечении десяти календарных дней после первого официального опубликования).

7. Для рассмотрения акта аттестационного обследования (далее - акт) создается Комиссия, положение и состав которой утверждаются приказом уполномоченного органа.

8. В состав комиссии входят представители:

1) органов национальной безопасности Республики Казахстан;

2) уполномоченного государственного органа по защите государственных секретов и обеспечения информационной безопасности;

3) уполномоченного органа.

9. Сведения о выданных аттестатах вносятся уполномоченным органом в реестр аттестатов, содержащий информацию о владельце ИС и разработчике ИС, наименовании ИС, реквизитах акта аттестационного обследования и аттестата, дате и основании переоформления аттестата, датах проведения и результатах дополнительных обследований, датах и основаниях отзыва/возврата аттестата, дате и основаниях прекращения действия аттестата.

Сноска. Пункт 9 в редакции постановления Правительства РК от 03.11.2011 № 1285 (вводится в действие по истечении десяти календарных дней после первого официального опубликования).

2. Порядок проведения аттестации

10. Аттестация осуществляется в следующем порядке:

1) заявителем подается заявка в уполномоченный орган по форме согласно приложению 1 к настоящим Правилам с предоставлением следующих документов:

заверенная подписью заявителя копия документа, удостоверяющего личность (для физических лиц);

заверенные подписью и печатью заявителя копии учредительных документов и справки либо свидетельства о государственной регистрации (перерегистрации)

юридического лица (для юридических лиц);

заверенные подписью и печатью заявителя копии нормативно-технических документов по ИБ аттестуемой ИС в составе согласно приложению 2 к настоящим Правилам;

утвержденный заявителем перечень технических и программных средств, входящих в состав аттестуемой ИС, по форме согласно приложениям 4 и 5 к настоящим Правилам;

утвержденная заявителем функциональная схема (план) взаимодействия компонентов ИС, а также интегрируемых компонентов ИС (физическая и логическая структура ИС, пояснительная записка к функциональной схеме);

проектная (программная) и предпроектная (технико-экономическое обоснование) документация на ИС;

2) уполномоченный орган в течение двух календарных дней с момента получения заявки осуществляет проверку соответствия заявки и прилагаемых к заявке документов требованиям к форме и комплектности, установленным настоящими Правилами;

3) в случае соответствия заявки и приложенных документов требованиям к форме и комплектности, установленным настоящими Правилами, заявка с приложенными документами в установленный в подпункте 2) пункта 10 настоящих Правил срок направляется уполномоченным органом в государственную техническую службу, в противном случае заявка возвращается заявителю с указанием причин возврата;

4) после получения заявки на проведение аттестации ИС государственная техническая служба в течение трех рабочих дней направляет заявителю два экземпляра договора на оказание услуг по аттестационному обследованию, договора на исполнение совместных работ по обеспечению информационной безопасности и при наличии в информационных системах средств криптографической защиты информации или при необходимости - договора на выполнение совместных секретных работ. Заявитель после получения двух экземпляров вышеуказанных договоров в течение трех рабочих дней подписывает и возвращает по одному экземпляру каждого договора в государственную техническую службу;

5) на основании договора, заключенного с заявителем, государственная техническая служба проводит аттестационное обследование ИС. Аттестационное обследование проводится в соответствии с нормативными правовыми актами и стандартами в области информационной безопасности, принятыми на территории Республики Казахстан, перечень которых определяется государственной технической службой с учетом примененных информационных технологий в аттестуемой ИС. Стоимость работ по проведению аттестационного

обследования определяется в соответствии с действующим законодательством Республики Казахстан;

6) заявитель обеспечивает доступ к помещению, оборудованию и информации по аттестуемой ИС для проведения аттестационного обследования государственной технической службой;

7) государственная техническая служба не допускает разглашения сведений, составляющих коммерческую или иную охраняемую законом тайну, ставшую известной при проведении работ по аттестационному обследованию ИС;

8) срок аттестационного обследования не должен превышать тридцати календарных дней с момента заключения договора на проведение аттестационного обследования. В случае, если структура аттестуемой ИС включает ведомственные или региональные компоненты ИС, государственная техническая служба обращается в уполномоченный орган с ходатайством о продлении срока аттестационного обследования с изложением причин невозможности соблюдения установленного срока. Уполномоченным органом принимается решение о продлении срока аттестационного обследования сроком не более тридцати календарных дней, о чем сообщается заявителю в течение трех календарных дней;

9) по результатам аттестационного обследования государственной технической службой составляется акт, который передается уполномоченному органу, составляется в четырех экземплярах (по одному для Комиссии, уполномоченного органа по защите государственных секретов, органов национальной безопасности и заявителя) и включает в себя сведения о фактическом состоянии защищенности ИС;

10) уполномоченный орган в течение двух календарных дней с момента получения акта созывает Комиссию и передает акт на рассмотрение Комиссии;

11) на основании акта Комиссией вырабатываются соответствующие рекомендации, которые оформляются в виде протокола. При рассмотрении данных акта Комиссия учитывает уровень функциональной сложности ИС и ее назначение, характер обрабатываемой ИС информации, категорию доступа ИС, режим обработки данных в ИС, комплектность нормативно-технической документации по информационной безопасности и соблюдение ее требований, оценку реальных угроз безопасности (потенциальные источники угроз и уязвимости);

12) на основании протокола Комиссии и с учетом акта уполномоченный орган в течение одного календарного дня принимает одно из следующих решений:

о выдаче или отказе в выдаче аттестата (решение об отказе в выдаче аттестата принимается на основании указанных в акте несоответствий требованиям

стандартов в области информационной безопасности, принятых на территории Республики Казахстан);

об устранении заявителем выявленных несоответствий (данное решение может быть принято не более одного раза к заявке на проведение аттестации ИС), копия решения направляется заявителю;

13) в случае принятия решения об устранении заявителем выявленных несоответствий, заявитель в течение двадцати рабочих дней с момента получения копии решения устраняет выявленные при аттестационном обследовании несоответствия и извещает уполномоченный орган об их устранении, после чего уполномоченный орган в течение трех рабочих дней извещает государственную техническую службу о необходимости проведения дополнительного аттестационного обследования ИС. Срок дополнительного обследования не должен превышать десяти рабочих дней со дня получения извещения из уполномоченного органа;

14) после проведения дополнительного аттестационного обследования осуществляются действия согласно подпунктам 9) - 12) пункта 10 настоящих Правил;

15) в случае принятия положительного решения по результатам аттестационного либо дополнительного аттестационного обследования уполномоченный орган в установленный в подпункте 12) пункта 10 настоящих Правил срок выдает аттестат по форме согласно приложению 3 к настоящим Правилам и вносит соответствующие сведения в реестр аттестатов. Представитель заявителя подтверждает получение аттестата под роспись;

16) реестр аттестатов имеет ограниченный доступ;

17) в случае отказа в выдаче аттестата уполномоченным органом в установленный в подпункте 12) пункта 10 настоящих Правил срок заявителю направляется соответствующее уведомление с указанием причин отказа.

Сноска. Пункт 10 в редакции постановления Правительства РК от 03.11.2011 № 1285 (вводится в действие по истечении десяти календарных дней после первого официального опубликования); с изменениями, внесенными постановлениями Правительства РК от 25.09.2012 № 1241 (вводится в действие по истечении десяти календарных дней со дня первого официального опубликования); от 28.01.2013 № 49 (вводится в действие по истечении десяти календарных дней со дня первого официального опубликования); от 21.05.2013 № 507 (вводится в действие по истечении десяти календарных дней со дня первого официального опубликования).

11. Аттестат выдается заявителю сроком на 3 года, с учетом неизменности условий функциональности системы, аппаратно-программного комплекса и информационных технологий, обеспечивающих обработку защищаемой

информации, определяющие безопасность информации (состав и структура технических средств, условия размещения, используемое программное обеспечение, режимы обработки информации, средства и меры защиты).

12. В случае изменения условий и технологии обработки информации, владельцы аттестованных ИС в течение пяти рабочих дней с момента таких изменений направляют в уполномоченный орган извещение с приложением описания произведенных изменений. В течение трех рабочих дней с момента получения извещения уполномоченный орган направляет в государственную техническую службу извещение с приложением описания произведенных изменений.

Сноска. Пункт 12 в редакции постановления Правительства РК от 28.01.2013 № 49 (вводится в действие по истечении десяти календарных дней со дня первого официального опубликования).

13. Государственная техническая служба в течение десяти рабочих дней с момента получения извещения от уполномоченного органа проводит дополнительное обследование ИС. В случае выявления изменений, которые могут нарушить уровень защищенности ИС, государственная техническая служба направляет уведомление в уполномоченный орган о необходимости переаттестации ИС, при отсутствии таких изменений государственная техническая служба направляет уполномоченному органу соответствующее уведомление.

Сноска. Пункт 13 в редакции постановления Правительства РК от 28.01.2013 № 49 (вводится в действие по истечении десяти календарных дней со дня первого официального опубликования).

14. Уполномоченный орган в течение трех рабочих дней с момента получения уведомления от государственной технической службы извещает заявителя аттестованной ИС о необходимости (отсутствие необходимости) переаттестации ИС. Переаттестация ИС осуществляется в порядке, установленном настоящими Правилами для проведения аттестации.

Сноска. Пункт 14 в редакции постановления Правительства РК от 28.01.2013 № 49 (вводится в действие по истечении десяти календарных дней со дня первого официального опубликования).

15. При утере аттестата владелец аттестованной ИС в течение трех рабочих дней с момента утери направляет в уполномоченный орган уведомление о его утере с указанием причин. Уполномоченный орган в течение пяти рабочих дней с момента получения уведомления выдает дубликат аттестата.

16. Уполномоченный орган принимает решение об отзыве аттестата в следующих случаях:

1) наличие письменного заявления заявителя;

2) выявление несогласованных с уполномоченным органом изменений в аттестованной ИС.

Сноска. Правила дополнены пунктом 16 в соответствии с постановлением Правительства РК от 03.11.2011 № 1285 (вводится в действие по истечении десяти календарных дней после первого официального опубликования).

17. Копия решения об отзыве аттестата направляется заявителю. Заявитель в течение трех рабочих дней с момента получения копии решения об отзыве аттестата возвращает аттестат уполномоченному органу.

В случае отзыва аттестата по основанию, предусмотренному подпунктом 2) пункта 16 настоящих Правил, заявитель в течение пятнадцати календарных дней с момента получения копии решения об отзыве аттестата принимает меры по устранению выявленных изменений.

Сноска. Правила дополнены пунктом 17 в соответствии с постановлением Правительства РК от 03.11.2011 № 1285 (вводится в действие по истечении десяти календарных дней после первого официального опубликования).

18. После устранения несоответствий, послуживших основанием для отзыва аттестата, заявитель представляет сведения об их устранении в уполномоченный орган для принятия решения о возврате аттестата.

Сноска. Правила дополнены пунктом 18 в соответствии с постановлением Правительства РК от 03.11.2011 № 1285 (вводится в действие по истечении десяти календарных дней после первого официального опубликования).

Приложение 1
к Правилам проведения аттестации государственных информационных систем и негосударственных информационных систем, интегрируемых с государственными информационными системами, на соответствие их требованиям информационной безопасности и принятым на территории Республики Казахстан стандартам

Кому_____
(наименование органа по аттестации)

ЗАЯВКА

на проведение аттестации государственной (негосударственной) информационной системы

_____

_____

(наименование заявителя, Ф.И.О. заявителя)

просит провести аттестацию

_____

_____

(наименование информационной системы)

на соответствие требованиям по информационной безопасности и принятым на территории Республики Казахстан стандартам.

1. Исходные данные по государственной (негосударственной) информационной системе на ____ листах прилагаются.

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

_____

(подпись, дата)

М.П.

Приложение 2
к Правилам проведения аттестации государственных информационных систем и негосударственных информационных систем, интегрируемых с государственными информационными системами, на соответствие их требованиям информационной безопасности и принятым на территории Республики Казахстан стандартам

ПЕРЕЧЕНЬ
нормативно-технических документов по информационной безопасности

Сноска. Перечень с изменением, внесенным постановлением Правительства РК от 03.11.2011 № 1285 (вводится в действие по истечении десяти календарных дней после первого официального опубликования).

1. Политика информационной безопасности заявителя.

2. Правила паспортизации средств вычислительной техники и использования информационных ресурсов.

3. Инструкция о парольной защите.

4. Инструкция о порядке действий пользователей во внештатных (кризисных) ситуациях.

5. Инструкция пользователя по эксплуатации компьютерного оборудования и программного обеспечения.

6. Инструкция по организации антивирусной защиты.

7. Инструкция о резервном копировании информации.

8. Инструкция по закреплению функций и полномочий администратора сервера.

9. Правила доступа пользователей и администраторов в серверные помещения.

10. Правила регистрации пользователей в корпоративной информационной сети.

11. Памятка для работы системных администраторов.

12. Памятка пользователю средств вычислительной техники.

13. Инструкция по использованию электронной почты и служб Интернет на рабочих станциях.

Приложение 3
к Правилам проведения аттестации государственных информационных систем и негосударственных информационных систем, интегрируемых с государственными информационными системами, на соответствие их требованиям информационной безопасности и принятым на территории Республики Казахстан стандартам

АТТЕСТАТ № _____
соответствия информационной системы требованиям информационной безопасности и принятым на территории Республики Казахстан стандартам

Сноска. Приложение 3 в редакции постановления Правительства РК от 03.11.2011 № 1285 (вводится в действие по истечении десяти календарных дней после первого официального опубликования).

_____
(указывается полное наименование ИС)

Действителен до "__" _____ 201_ г. № ____

1. Настоящим аттестатом удостоверяется, что:

_____
(полное наименование ИС)

соответствует информационной безопасности и принятым на территории Республики Казахстан стандартам.

Состав комплекса технических средств ИС (с указанием заводских номеров, модели, изготовителя), перечень используемых программных средств, а также средств защиты ИС (с указанием изготовителя) прилагаются.

2. С учетом результатов аттестационного обследования на ИС разрешается обработка _____ информации.
(служебная, конфиденциальная и т.п.)

3. При эксплуатации ИС запрещается:

(указываются ограничения, которые могут повлиять на эффективность мер и средств защиты информации)

4. Контроль за эффективностью реализованных мер и средств защиты возлагается на соответствующие подразделения Заявителя.

5. Подробные результаты аттестационного обследования приведены в акте аттестационного обследования (№ ____ "_____" 201__ г.) и отчете к акту аттестационного обследования.

6. Аттестат выдан на три года, в течение которых должна быть обеспечена неизменность условий функционирования ИС.

7. Перечень характеристик, об изменениях которых требуется обязательно извещать государственную техническую службу:

Сноска. Пункт 7 в редакции постановления Правительства РК от 28.01.2013 № 49 (вводится в действие по истечении десяти календарных дней со дня первого официального опубликования).

7.1 _____

7.2 _____

Председатель **(Ф.И.О.)**

М П

"____" _____ 20__ г.

Приложение 4
к Правилам проведения аттестации государственных информационных систем и негосударственных информационных систем, интегрируемых с государственными информационными системами, на соответствие их требованиям информационной безопасности и принятым на территории Республики Казахстан стандартам

Перечень технических средств

Сноска. Правила дополнены приложением 4 в соответствии с постановлением Правительства РК от 03.11.2011 № 1285 (вводится в действие по истечении десяти календарных дней после первого официального опубликования).

№ п\п	Производитель, модель	Серийный/ инвен-	Номер сертифи-	Физическое	Тип (согласно технической	Основное функциональное назначение (согласно программ-	Используемые методы	Разработчик, названи версия (встроенного програ

		тарный номер	ката по ИБ (при наличии)	место-располо-жение	докумен-тации)	н о й докумен-т а ц и и к ИС)	защиты информации	н о г о обеспе ния)
1	2	3	4	5	6	7	8	9

Приложение 5
к Правилам проведения аттестации государственных информационных систем и негосударственных информационных систем, интегрируемых с государственными информационными системами, на соответствие их требованиям информационной безопасности и принятым на территории Республики Казахстан стандартам

Перечень программных средств

Сноска. Правила дополнены приложением 5 в соответствии с постановлением Правительства РК от 03.11.2011 № 1285 (вводится в действие по истечении десяти календарных дней после первого официального опубликования).

№ п\ п	Разра-ботчик	Название	Версия	Место установки (из перечня технических средств)	Тип (согласно программной документации)	Основное функциональное назначение (согласно программной документации)	Используем методы защиты информации
1	2	3	4	5	6	7	8