

О внесении изменений и дополнений в постановление Правительства Республики Казахстан от 30 декабря 2009 года № 2280 "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 3 ноября 2011 года № 1285. 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).

Правительство Республики Казахстан **ПОСТАНОВЛЯЕТ:**

1. Внести в постановление Правительства Республики Казахстан от 30 декабря 2009 года № 2280 "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" (САПП Республики Казахстан, 2010 г., № 4, ст. 39) следующие изменения и дополнения:

в Правилах 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, утвержденных указанным постановлением:

пункт 1 изложить в следующей редакции:

"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).";

подпункт 5) пункта 2 изложить в следующей редакции:

"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. ";

дополнить пунктом 6-1 следующего содержания:

"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. ";

пункты 9 и 10 изложить в следующей редакции:

"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.

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 свидетельства о государственной регистрации 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 трех рабочих 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 уполномоченную организацию, в противном случае заявка возвращается заявителю с указанием причин возврата;

4) после получения заявки на проведение аттестации ИС уполномоченная организация 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 уполномоченную организацию;

5) на основании договора, заключенного с заявителем, уполномоченная организация 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 уполномоченной организацией 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 уполномоченной организацией;

7) уполномоченная организация 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, уполномоченная организация 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 уполномоченной организацией составляется акт, который передается уполномоченному органу. Акт 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 десяти рабочих 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 пяти рабочих дней принимает одно из следующих решений:

о выдаче или об 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 уполномоченную организацию 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

П р а в и л ;

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.;

в пункте 14 слова "владельцев ИС" заменить словами "заявителя, аттестованной ИС";

дополнить пунктами 16, 17 и 18 следующего содержания:

"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.

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.

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

приложение 2 к указанным Правилам дополнить пунктом 13 следующего содержания :

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

приложение 3 к указанным Правилам изложить в новой редакции согласно приложению 1 к настоящему постановлению;

дополнить приложениями 4 и 5 к указанным Правилам согласно приложениям 2 и 3 к настоящему постановлению.

2. Настоящее постановление вводится в действие по истечении десяти календарных дней после первого официального опубликования.

Премьер - Министр

Республики Казахстан

К. Масимов

Приложение 1

к постановлению

Правительства

Республики Казахстан

от 3 ноября 2011 года № 1285

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**

(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 уполномоченную организацию в области информатизации:

7.1 _____

7.2 _____

Председатель

(Ф.И.О.)

М П

"___" _____ 20__ г.

Приложение 2

к постановлению
Республики Казахстан

Правительства

от 3 ноября 2011 года № 1285

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

№ п/п	Производитель, модель	Серийный/инвентарный номер	Номер сертификата по ИБ (при наличии)	Физическое местоположение	Тип (согласно технической документации)	Основное функциональное назначение (согласно программной документации ИС)	Используемые методы защиты информации	Разработчик, название версии (встроенного программного обеспечения)
1	2	3	4	5	6	7	8	9

Приложение 3
к постановлению
Республики Казахстан
от 3 ноября 2011 года № 1285
Правительства

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

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

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