Об утверждении Инструкции по подтверждению соответствия информационных систем, технических, программно-технических и программных средств (изделий) , технических средств защиты информации требованиям информационной безопасности

Утративший силу

Приказ Руководителя Канцелярии Премьер-Министра Республики Казахстан от 14 июня 2013 года N 25-1-21. Зарегистрирован в Министерстве юстиции Республики Казахстан 2 июля 2013 года N 8543. Утратил силу приказом Руководителя Канцелярии Премьер-Министра Республики Казахстан от 15 марта 2021 года № 10-4-10.

Сноска. Утратил силу приказом Руководителя Канцелярии Премьер-Министра РК от 15.03.2021 № 10-4-10 (вводится в действие по истечении десяти календарных дней после дня его первого официального опубликования).

В соответствии с Законом Республики Казахстан 9 ноября 2004 года «О техническом регулировании» и подпунктом 21) пункта 12 Положения о Канцелярии Премьер-Министра Республики Казахстан, утвержденного постановлением Правительства Республики Казахстан от 11 сентября 2002 года № 993, **ПРИКАЗЫВАЮ**:

1. Утвердить прилагаемую Инструкцию по подтверждению соответствия информационных систем, технических, программно- технических и программных средств (изделий), технических средств защиты информации требованиям информационной безопасности.

2. Признать утратившим силу Приказ Руководителя Канцелярии Премьер-Министра Республики Казахстан от 3 октября 2005 года № 25-1-90 «Об утверждении Правил обязательного подтверждения соответствия информационных систем, технических, программно- технических и программных средств (изделий), технических средств защиты информации требованиям информационной безопасности» (зарегистрирован в Реестре государственной регистрации нормативных правовых актов № 3923).

3. Настоящий приказ вводится в действие со дня государственной регистрации в Министерстве юстиции Республики Казахстан.

Руководитель Канцелярии **Е. Кошанов**

Утверждена
приказом Руководителя Канцелярии
Премьер-Министра
Республики Казахстан
от 14 июня 2013 года № 25-1-21

Инструкция по подтверждению соответствия информационных систем, технических, программно-технических и программных средств (изделий), технических средств защиты информации требованиям информационной безопасности

1. Общие положения

1. Настоящая Инструкция по подтверждению соответствия информационных систем, технических, программно-технических и программных средств (изделий) , технических средств защиты информации требованиям информационной безопасности (далее - Инструкция) разработана в соответствии со следующими нормативными правовыми актами:

Законом Республики Казахстан от 9 ноября 2004 года «О техническом регулировании»;

Законом Республики Казахстан от 6 января 2012 года «О национальной безопасности Республики Казахстан»;

Законом Республики Казахстан 11 января 2007 года «Об информатизации»;

Законом Республики Казахстан 7 января 2003 года «Об электронном документе и электронной цифровой подписи».

2. В Инструкции используются понятия и определения по вопросам подтверждения соответствия в соответствии с Законом Республики Казахстан от 9 ноября 2004 года «О техническом регулировании».

3. Инструкция детализирует организацию и проведение подтверждения соответствия информационных систем, технических, программно-технических и программных средств (изделий), технических средств защиты информации (далее - СЗИ и СВТ) требованиям информационной безопасности (далее - подтверждение соответствия). При подтверждении соответствия подтверждается соответствие СЗИ и СВТ требованиям нормативных правовых актов, конкретных стандартов в области информационной безопасности, в том числе по вопросам применения технических средств защиты информации, согласованными с уполномоченным государственным органом по защите государственных секретов и обеспечению информационной безопасности, органами национальной безопасности и другими заинтересованными государственными органами.

4. Подтверждению соответствия требованиям информационной безопасности подлежат СЗИ и СВТ, включенные в Перечень продукции и услуг, подлежащих

обязательной сертификации, утвержденным постановлением Правительства Республики Казахстан от 20 апреля 2005 года № 367.

Средства криптографии (шифрования), входящие в состав СЗИ и СВТ, подлежат подтверждению соответствия в форме сертификации в соответствии с отдельными правилами подтверждения соответствия шифровальных средств требованиям информационной безопасности, утверждаемыми в установленном порядке.

Технические средства обработки, передачи и хранения информации, составляющей государственные секреты, подлежат подтверждению соответствия в форме сертификации в порядке, определенном разделом 7 настоящей Инструкции.

5. Процедуры подтверждения соответствия проводят исключительно органы по подтверждению соответствия (Орган) и испытательные лаборатории (центры), аккредитованные на право проведения таких испытаний.

Органы по подтверждению соответствия и испытательные лаборатории (центры), осуществляющие работы по подтверждению соответствия СЗИ и СВТ требованиям информационной безопасности обеспечивают неразглашение сведений, предоставляемых заявителями, либо полученных в ходе проведения подтверждения соответствия.

6. Условия неразглашения предоставляемых сведений определяются в договоре, заключаемом между заявителем или собственником сведений и органом по подтверждению соответствия или испытательной лабораторией (центром), и в соответствии с законодательством Республики Казахстан о государственных секретах.

7. Конкретные перечни сведений, в том числе СЗИ и СВТ, составляющих государственные секреты Республики Казахстан, условия и порядок их передачи органу по подтверждению соответствия и/или испытательной лаборатории (центру) в целях проведения подтверждения соответствия СЗИ и СВТ, определяются в соответствии с законодательством Республики Казахстан о государственных секретах и указываются в договорах на проведение совместных секретных работ.

8. Органы по подтверждению соответствия и испытательные лаборатории (центры), осуществляющие работы по подтверждению соответствия используемых в государственных органах СЗИ и СВТ, должны иметь разрешение Комитета национальной безопасности Республики Казахстан на проведение работ с использованием сведений, составляющих государственные секреты Республики Казахстан.

2. Подтверждение соответствия СЗИ и СВТ требованиям информационной безопасности

9. Под подтверждением соответствия СЗИ и СВТ требованиям информационной безопасности понимается процедура, результатом которой является документальное удостоверение соответствия СЗИ и СВТ требованиям информационной безопасности органом по подтверждению соответствия в виде сертификата соответствия требованиям, установленным техническими регламентами, положениями стандартов.

10. Подтверждение соответствия СЗИ и СВТ требованиям информационной безопасности проводится в соответствии с требованиями нормативных документов, устанавливающих параметры и методы проведения подтверждения соответствия и испытаний в зависимости от степени секретности обрабатываемой (хранимой) информации.

11. С учетом степени секретности обрабатываемой (хранимой) информации, данные из состава сертификатов соответствия СЗИ и СВТ требованиям информационной безопасности используются в установленном порядке для внесения в предписания на эксплуатацию СЗИ и СВТ (по требованиям информационной безопасности).

Пользователи СЗИ и СВТ, имеющих сертификат соответствия, обеспечивают выполнение действующих предписаний на эксплуатацию (по требованиям информационной безопасности). При этом рекомендуемый порядок создания СЗИ и СВТ, подлежащих подтверждению соответствия требованиям информационной безопасности, осуществляется согласно приложению к настоящей Инструкции.

3. Проведение работ по подтверждению соответствия требованиям информационной безопасности

12. Подтверждение соответствия СЗИ и СВТ требованиям информационной безопасности предусматривает следующую последовательность процедур:

подача лицом заявления о проведении работ по сертификации (далее - заявитель) в орган по подтверждению соответствия заявки о проведении сертификации СЗИ или СВТ;

принятие органом по подтверждению соответствия решения по результатам рассмотрения заявки;

выбор схемы подтверждения соответствия совместно с заявителем;

заключение между органом по подтверждению соответствия и заявителем договора на проведение работ по сертификации;

проведение идентификации, отбора образца (образцов) заявленных СЗИ или СВТ;

анализ результатов испытаний;

принятие решения о выдаче сертификата соответствия;

регистрация сертификата соответствия в реестре государственной системы технического регулирования и выдача его заявителю;

осуществление инспекционного контроля за сертифицированной продукцией (если это предусмотрено схемой сертификации);

предоставление информации о результатах сертификации.

13. К заявке, в зависимости от типа заявленного СЗИ и СВТ и выбранной схемы сертификации, прилагаются следующие сопроводительные документы:

учредительные документы заявителя;

инвойс, контракт на поставку СЗИ и СВТ (при импорте);

накладная на предъявляемую партию образцов заявленного СЗИ и СВТ;

техническое описание СЗИ и СВТ, содержащее технические параметры, позволяющие идентифицировать СЗИ и СВТ и оценить соответствие СЗИ и СВТ установленным требованиям;

документ изготовителя, подтверждающий факт производства им заявляемого для подтверждения соответствия СЗИ и СВТ (в случае, если заявитель является продавцом);

о возможности отбора образцов для проведения испытаний;

оценка технических характеристик СЗИ или СВТ уполномоченным государственным органом по защите государственных секретов и обеспечению информационной безопасности (СЗИ) и уполномоченным органом в сфере информатизации (СВТ);

нормативные или технические документы, содержащие требования к подтверждаемым показателям СЗИ и СВТ, методы испытаний;

исходные коды программ, реализующих функции СЗИ и СВТ, в том числе, механизмы обработки и защиты информации.

Техническое описание СЗИ и СВТ должно содержать:

наименование, назначение, комплектность СЗИ и СВТ, выполняемые ими функции;

версию программного обеспечения (при наличии);

электрические характеристики, характеристики радиоизлучения (для радиоэлектронных средств);

условия применения в сети передачи данных общего пользования; схемы подключения к сети передачи данных общего пользования с указанием реализуемых интерфейсов и протоколов;

сведения о наличии (отсутствии) встроенных средств криптографии (шифрования), приемников глобальных спутниковых навигационных систем;

условия эксплуатации, включая климатические и механические требования, способы размещения, типы электропитания.

14. Заявка и сопроводительная документация к ней представляются на государственном, русском и/или английском языках. В случае наличия перевода с иностранного языка, заявителем представляется подтверждение его аутентичности.

В предоставляемой заявителем в орган по подтверждению соответствия нормативной и технической документации должно быть дано полное описание всех функций и механизмов обработки и защиты информации, реализованных в данной информационной системе.

15. Заявка и (или) документы, приложенные к ней, не соответствующие требованиям пунктов 13 и 14 настоящей Инструкции, возвращается заявителю с указанием причин возврата в сроки, предусмотренные для рассмотрения заявки.

При отсутствии замечаний (после устранения замечаний) орган по подтверждению соответствия направляет заявителю решение по результатам рассмотрения заявки.

В случае если заявитель согласен с условиями процедур подтверждения соответствия, заключается договор на проведение данных работ.

16. При рассмотрении заявки устанавливается:

наличие учредительных документов заявителя;

полнота представленной документации.

17. В ходе предварительного рассмотрения заявки орган по подтверждению соответствия:

информирует заявителя о порядке и процедурах подтверждения соответствия, нормативных требованиях, на соответствие которым будут проводиться работы по подтверждению соответствия;

разъясняет заявителю, какие могут быть установлены ограничения при выдаче сертификата соответствия;

направляет заявителю письменное уведомление с перечнем недостатков, которые были обнаружены в ходе рассмотрения заявки, и рекомендации по их устранению;

отказывает заявителю в проведении работ по подтверждению соответствия.

Причинами отказа являются:

представление документации, не соответствующей заявленным СЗИ и СВТ;

утрата силы нормативных или технических документов, содержащих требования к подтверждаемым показателям заявленного СЗИ или СВТ на момент подачи заявки;

отсутствие в нормативной или технической документации на заявленные СЗИ или СВТ методов испытаний, содержащих требования к показателям, подтверждаемым при проведении работ по подтверждению соответствия, или неполное их изложение;

несоответствие показателей, изложенных в нормативной или технической документации и подтверждаемых при проведении работ по подтверждению соответствия заявленного СЗИ или СВТ, требованиям нормативных документов. В случае отказа в удовлетворении заявки орган по подтверждению соответствия вместе с решением в течение 10 календарных дней официально направляет заявителю все представленные им документы. К решению прилагается мотивированный отказ в подтверждении соответствия заявленного СЗИ и СВТ требованиям информационной безопасности.

4. Проведение отбора и идентификации образцов СЗИ и СВТ

18. Идентификация заявленного СЗИ или СВТ, отбор необходимого количества образцов (образца) и, если нормативными и техническими документами предусмотрены упаковка и маркировка, проверка их наличия и состояния осуществляются специалистом органа по подтверждению соответствия, работником испытательной лаборатории (центра) в присутствии представителя заявителя. По поручению органа по подтверждению соответствия отбор образцов проводит компетентная комиссия из представителей незаинтересованных организаций, назначенная заявителем.

Количество отбираемых образцов СЗИ или СВТ, методика их отбора, а также условия их транспортировки и хранения должны соответствовать требованиям нормативных документов по подтверждению соответствия на заявленные СЗИ или СВТ.

Отбор образцов СЗИ или СВТ оформляется актом в двух экземплярах. Результаты идентификации образцов СЗИ или СВТ заносятся в акт отбора.

Отобранные образцы пломбируются (если это возможно) в присутствии заявителя и направляются в аккредитованную испытательную лабораторию (центр), с приложением акта отбора образцов продукции и технической документации к ним.

5. Сертификационные испытания образцов СЗИ или СВТ требованиям информационной безопасности

19. Сертификационные испытания требованиям информационной безопасности отобранных образцов заявленного СЗИ или СВТ согласно договору на выполнение работ по подтверждению соответствия производится аккредитованной испытательной лабораторией (центром) согласно программе испытаний.

20. При подтверждении соответствия СЗИ или СВТ в форме проведения сертификации применяются следующие схемы сертификации:

схема № 2 - применяется при сертификации СЗИ или СВТ по заявке заявителя и предусматривает сертификационные испытания образцов, взятых у заявителя, анализ состояния производства и инспекционную проверку за

сертифицированными СЗИ или СВТ в течение срока действия сертификата соответствия. Сертификат соответствия выдается сроком на 1 год;

схема № 3 - применяется при сертификации СЗИ или СВТ по заявке изготовителя и предусматривает сертификационные испытания образцов, взятых у изготовителя, анализ состояния производства и инспекционную проверку за сертифицированными СЗИ или СВТ в течение срока действия сертификата соответствия. Сертификат соответствия выдается сроком на 1 год;

схема № 5 - применяется при сертификации СЗИ или СВТ по заявке изготовителя и предусматривает проведение сертификационных испытаний образцов, взятых у изготовителя, и контроль за возможностью изготовителя выпускать в течение срока действия сертификата соответствия СЗИ или СВТ, соответствующие установленным требованиям. Инспекционная проверка сертифицированных СЗИ или СВТ осуществляется в течение всего срока действия сертификата соответствия. Сертификат соответствия выдается сроком на 3 года;

схема № 7 - применяется для сертификации партии изготовленных СЗИ или СВТ по заявке изготовителя или заявителя и предусматривает сертификационные испытания образцов, взятых из этой партии. Сертификат соответствия выдается с указанием идентификационных признаков СЗИ или СВТ, входящих в представленную партию, и выдается сроком до 3 лет.

Подтверждение соответствия в форме проведения сертификации СЗИ или СВТ должно осуществляться в течение 2 месяцев с даты заключения договора о проведении работ по подтверждению соответствия. При проведении подтверждения соответствия сложного оборудования СЗИ или СВТ срок может быть увеличен до 4 месяцев.

Указанные схемы не распространяются на порядок проведения сертификации технических средств обработки, передачи и хранения информации, составляющей государственные секреты, особенности которого определяются разделом 7 настоящей Инструкции.

21. Сертификационные испытания проводятся аккредитованной в установленном порядке испытательной лабораторией (центром) с учетом вида СЗИ и СВТ на соответствие установленным в нормативной документации требованиям информационной безопасности.

22. По результатам испытаний образцов заявленного СЗИ или СВТ испытательной лабораторией (центром) составляется протокол, направляется в орган по подтверждению соответствия и заявителю.

В зависимости от схемы сертификации производится анализ состояния производства продукции.

Орган по подтверждению соответствия после анализа протоколов испытаний, оценки производства и других документов о соответствии продукции, осуществляет оценку соответствия продукции установленным требованиям. Результаты этой оценки отражают в заключении эксперта. На основании данного заключения Орган принимает решение о выдаче сертификата соответствия, оформляет и регистрирует его в реестре выданных сертификатов соответствия либо мотивированного отказа в выдаче сертификата соответствия.

6. Выдача документального удостоверения

23. При положительном решении орган по подтверждению соответствия оформляет и выдает сертификат соответствия согласно нормативным документам по стандартизации. Копия сертификата соответствия выдается по запросу заявителя.

Действие сертификата соответствия начинается с даты его выдачи, указанной в реестре выданных сертификатов соответствия.

24. Отказ в выдаче, приостановление или прекращение действия, отзыв или аннулирование документального удостоверения осуществляется в соответствии с законодательством Республики Казахстан о техническом регулировании.

25. Приобретенное в период действия сертификата соответствия СЗИ или СВТ используются на всей территории Республики Казахстан в течение всего срока годности (службы) СЗИ или СВТ в соответствии с областью применения.

26. Держатель сертификата соответствия:

обеспечивает соответствие установленным требованиям СЗИ или СВТ, на которые выданы сертификаты соответствия;

обеспечивает беспрепятственное выполнение своих полномочий представителями органа по подтверждению соответствия и лицами, выполняющими инспекционную проверку сертифицированных СЗИ или СВТ;

прекращает реализацию СЗИ или СВТ, если срок действия сертификата соответствия истек, либо действие сертификата соответствия прекращено или приостановлено.

27. Орган по подтверждению соответствия осуществляет инспекционную проверку сертифицированных СЗИ или СВТ, если это предусмотрено схемой сертификации.

Инспекционная проверка сертифицированных СЗИ или СВТ осуществляется не реже одного раза в год.

Периодичность, сроки и объем инспекционной проверки определяются программой, согласованной органом по подтверждению соответствия и держателем сертификата соответствия.

28. Орган по подтверждению соответствия оформляет по результатам инспекционной проверки заключение о соответствии или несоответствии СЗИ

или СВТ установленным требованиям, о чем информирует держателя сертификата соответствия, в случае приостановлении действия или отмене действия сертификата соответствия информирует также уполномоченный орган в области технического регулирования и других заинтересованных лиц.

7. Сертификационные испытания технических средств, предназначенных для обработки, передачи и хранения информации, составляющей государственные секреты, требованиям информационной безопасности

29. Сертификационным испытаниям на соответствие требованиям информационной безопасности подвергаются все заявленные технические средства, предназначенные для обработки, передачи и хранения информации, составляющей государственные секреты (далее - ТС).

30. Срок действия сертификатов соответствия на сертифицированные ТС составляет три года со дня их выдачи. При изменении состава комплектующих узлов и блоков, ТС подлежит повторной сертификации.

31. В результате сертификационных испытаний на соответствие требованиям норм по каналу побочных электромагнитных излучений (далее - ПЭМИ) должна производиться классификация ТС по категориям объектов СВТ, путем сравнения результатов расчета зон радиотехнической безопасности с требованиями, установленными Инструкцией по обеспечению режима секретности при обработке сведений, составляющих государственные секреты, с применением средств вычислительной техники, утвержденной приказом Руководителя Канцелярии Премьер-Министра Республики Казахстан от 29 июля 2004 года № 25-1-59 с, зарегистрированным в Реестре государственной регистрации нормативных правовых актов на № 2993 (далее - Инструкция).

По результатам классификации ТС сертификационным органом выдаются рекомендации о категории объекта СВТ, на котором может применяться ТС.

32. Для расчета зон радиотехнической безопасности применяются нормы и методики, определяемые уполномоченным государственным органом по защите государственных секретов по согласованию с Комитетом национальной безопасности. Разработка методики осуществляется сертификационными органами и согласовываются с Комитетом национальной безопасности Республики Казахстан.

33. При необходимости, определяемой заявителем, в ходе сертификации ТС кроме испытаний на соответствие требованиям информационной безопасности по каналу ПЭМИ, проводятся испытания на наличие каналов акустоэлектрических преобразований (микрофонный эффект), параметрических каналов (паразитная модуляция побочных излучений), каналов высокочастотного навязывания и облучения и др.

34. В ходе работ по подтверждению соответствия ТС также необходимо осуществлять ведение электронно-компонентной базы проверенных технических средств, в которой должны содержаться сведения об узлах и блоках входящих в состав технических средств, включая их фото-и (или) рентгеснимки.

В случае запросов заинтересованных государственных органов (КНБ, КПМ, СВР РК «Сырбар» и др.) сертификационные органы предоставляют в их адрес информацию из указанной базы данных.

35. Программное обеспечение ТС обработки информации, составляющей государственные секреты, должно подвергаться отдельной сертификации по требованиям стандартов информационной безопасности в соответствии с высокими уровнями доверия.

36. После проведения сертификационных испытаний все узлы и блоки комплектующих технических средств опечатываются специальными наклейками с указанием наименования проверявшей организации и уникальным номером, к которому должна осуществляться привязка базы данных о сертифицированных технических средствах, с включением в нее протоколов измерений и электронно-компонентной базы. На наклейках ТС, предназначенных для обработки секретной информации, должна быть указана наивысшая категория объекта СВТ на котором рекомендуется его использование. Например - « Сертифицировано по 3 категории».

37. Сертификат соответствия ТС либо его приложение должны содержать следующие сведения:

категория объекта СВТ, на котором рекомендовано применение ТС;

результаты расчетов зон радиотехнической безопасности по 1,2 и 3 категории;

рекомендации об ограничениях по использованию ТС, связанных с выявленными каналами утечки, указанными в пункте 36 настоящей Инструкции.

38. Сертификация технических средств защиты секретной информации осуществляется путем подтверждения соответствия требованиям, заявленным в технических паспортах.

Приложение
к Инструкции по подтверждению
соответствия информационных систем,
технических, программно-технических
и программных средств (изделий),
технических средств защиты информации
требованиям информационной безопасности

Рекомендуемый порядок
создания СЗИ и СВТ, подлежащих подтверждению
соответствия требованиям информационной безопасности

1. Создание СЗИ и СВТ, подлежащих подтверждению соответствия требованиям информационной безопасности, включает следующие этапы:

разработка, согласование и утверждение технического задания на информационную систему;

разработка и утверждение проектно-сметной документации на информационную систему;

реализация согласованных проектных решений;

проведение конкурса на разработку информационной системы в соответствии с утвержденными техническим заданием и проектно-сметной документацией;

разработка информационной системы в соответствии с утвержденными техническим заданием и проектно-сметной документацией;

внедрение информационной системы в соответствии с утвержденными техническим заданием и проектно-сметной документацией;

проведение отраслевой оценки информационной системы уполномоченным органом в сфере информатизации и связи в соответствии с его нормативными документами.

2. Техническое задание и проектно-сметная документация на разработку СЗИ и СВТ требованиям информационной безопасности в обязательном порядке согласовывается с уполномоченным государственным органом по защите государственных секретов и обеспечению информационной безопасности, уполномоченным органом в сфере информатизации, органами национальной безопасности.