ГОСУДАРСТВЕННЫЙ СТАНДАРТ РЕСПУБЛИКИ КАЗАХСТАН

Защита информации

ПОРЯДОК СОЗДАНИЯ АВТОМАТИЗИРОВАННЫХ СИСТЕМ В ЗАЩИЩЕННОМ ИСПОЛНЕНИИ

Общие положения

СТ РК 34.025-2006

Издание официальное

Комитет по техническому регулированию и метрологии Министерства индустрии и торговли Республики Казахстан (Госстандарт)

Астана

Предисловие

1 РАЗРАБОТАН И ВНЕСЕН ТОО «Специальное конструкторско-технологическое бюро «Гранит»

2 УТВЕРЖДЕН И ВВЕДЕН В ДЕЙСТВИЕ Приказом Председателя Комитета по техническому регулированию и метрологии Министерства индустрии и торговли Республики Казахстан от 15 декабря 2006 г. № 550

3 Настоящий стандарт разработан с учетом основных положений стандарта Российской Федерации ГОСТ Р 51583-2000 «Защита информации. Порядок создания автоматизированных систем в защищенном исполнении. Общие положения»

4 В настоящем стандарте реализованы нормы законов Республики Казахстан О техническом регулировании, О языках в Республике Казахстан, Об информатизации, О государственных секретах, Соглашения Всемирной торговой организации по техническим барьерам в торговле, Концепция информационной безопасности Республики Казахстан, Постановление КМ РК № 1111-43с 05.11.94 «Об утверждении Положения о государственной системе защиты информации РК», Постановление Правительства Республики Казахстан от 19 октября 2000 года N 1561 Об утверждении Правил выдачи сертификата соответствия технических средств защиты сведений, составляющих государственные секреты

5 СРОК ПЕРВОЙ ПРОВЕРКИ 2011 год
ПЕРИОДИЧНОСТЬ ПРОВЕРКИ 5 лет

6 ВВЕДЕН ВПЕРВЫЕ

ГОСУДАРСТВЕННЫЙ СТАНДАРТ РЕСПУБЛИКИ КАЗАХСТАН

Защита информации
ПОРЯДОК СОЗДАНИЯ АВТОМАТИЗИРОВАННЫХ СИСТЕМ В ЗАЩИЩЕННОМ ИСПОЛНЕНИИ
Общие положения

Дата введения 2008.01.01

1 Область применения

Настоящий стандарт распространяется на автоматизированные системы в защищенном исполнении, используемые в различных видах деятельности (исследования, управление, проектирование, производство и т. п.), включая их сочетания, в процессе создания и применения которых осуществляется обработка защищаемой информации, содержащей сведения, отнесенные к государственным секретам (далее – секретная информация, если степень ее секретности не оговаривается особо).

Настоящий стандарт устанавливает дополнительные требования и положения стандартов класса 34 "Информационная технология. Комплекс стандартов на автоматизированные системы" в части порядка создания и применения автоматизированных систем в защищенном исполнении.

Настоящий стандарт применяется на территории Республики Казахстан органами государственной власти, местного самоуправления, организациями, предприятиями и учреждениями независимо от их организационно-правовой формы и формы собственности, которые заказывают, разрабатывают, изготавливают и используют (эксплуатируют) автоматизированные системы в защищенном исполнении.

2 Нормативные ссылки

В настоящем стандарте использованы ссылки на следующие стандарты:

СТ РК 34.012-2002 Информационная технология. Сертификация программных средств. Типовая методика оценки качества программной документации.

СТ РК 34.014-2002 Информационная технология. Комплекс стандартов на автоматизированные системы. Автоматизированные системы. Термины и определения.

СТ РК 34.015-2002 Информационная технология. Комплекс стандартов на автоматизированные системы. Техническое задание на создание автоматизированной системы.

СТ РК 34.026-2006 Защита информации. Термины и определения.

СТ РК 1170-2004 Защита информации. Нормы защиты речевой информации, циркулирующей в служебном помещении, от утечки по акустическому (речевому) и вибрационным каналам.

СТ РК 1200-2002 Государственная система защиты информации. Требования к техническим средствам защиты информации, используемых в государственных учреждениях.

СТ РК 1202-2002 Государственная система защиты информации. Общие требования к техническим средствам защиты информации. Основные положения.

СТ РК ГОСТ Р 50739-2006 Средства вычислительной техники. Защита от несанкционированного доступа к информации. Общие технические требования.

Издание официальное

СТ РК ГОСТ Р 51275-2006 Защита информации. Объект информатизации. Факторы, воздействующие на информацию.

ГОСТ 34.201-89 Информационная технология. Комплекс стандартов на автоматизированные системы. Виды, комплектность и обозначение документов при создании автоматизированных систем.

ГОСТ 34.601-90 Информационная технология. Комплекс стандартов на автоматизированные системы. Автоматизированные системы. Стадии создания.

ГОСТ 16504-81 Система государственных испытаний продукции. Испытания и контроль качества продукции. Основные термины и определения.

3 Термины, определения и сокращения

В настоящем стандарте применяют следующие термины с соответствующими определениями.

3.1 **Автоматизированная система:** Организационно-техническая система, представляющая собой совокупность следующих взаимосвязанных компонентов: технических средств обработки и передачи информации (вычислительной техники и связи), методов и алгоритмов обработки в виде соответствующего программного обеспечения, данных на различных носителях, персонала и пользователей, объединенных по организационно-структурному, тематическому, технологическому или другим признакам для выполнения автоматизированной обработки данных (СТ РК 34.012).

3.2 **Автоматизированная система в защищенном исполнении:** Автоматизированная система, реализующая информационную технологию выполнения установленных функций в соответствии с требованиями стандартов и/или нормативных документов по защите информации.

3.3 **Аттестация автоматизированной системы в защищенном исполнении**: Процесс комплексной проверки выполнения заданных функций автоматизированной системы по обработке защищаемой информации на соответствие требованиям стандартов и/или нормативных документов в области защиты информации и оформления документов о ее соответствии выполнять функции по обработке защищаемой информации на конкретном объекте информатизации.

3.4 **Государственные секреты**: Защищаемые государством сведения, составляющие государственную и служебную тайны, распространение которых ограничивается государством с целью осуществления эффективной военной, экономической, научно-технической, внешнеэкономической, внешнеполитической, разведывательной, контрразведывательной, оперативно-розыскной и иной деятельности, не вступающей в противоречие с общепринятыми нормами международного права [1].

3.5 **Защита информации**: Организационные, правовые технические и технологические мероприятия, проводимые в целях предотвращения утечки, хищения, утраты, несанкционированного уничтожения, изменения, модификации (подделки), несанкционированного копирования, блокирования доступа к информации [2].

3.6 **Защищаемая информация**: Информация, являющаяся предметом собственности и подлежащая защите в соответствии с требованиями правовых документов или требованиями, устанавливаемыми собственником информации (СТ РК 1202).

3.7 **Закладное устройство**: Элемент средства съема информации, скрытно внедряемый (закладываемый или вносимый) в места возможного съема информации (в том числе в ограждение, конструкцию, оборудование, предметы интерьера, транспортные средства, а также в технические средства и системы обработки информации) (СТ РК ГОСТ Р 51275).

3.8 **Информационная сфера**: Сфера деятельности субъектов, связанная с созданием, преобразованием и потреблением информации [3].

3.9 **Информационная технология**: Приемы, способы и методы применения технических и программных средств при выполнении функций обработки информации (СТ РК 1200).

3.10 **Информационный процесс**: Процесс создания, сбора, обработки, накопления, хранения, поиска, передачи, использования и распространения информации с использованием информационных технологий [4].

3.11 **Испытания**: Экспериментальное определение количественных и/или качественных характеристик свойств объекта испытаний от воздействий на него при его функционировании или при моделировании объекта и/или воздействий (ГОСТ 16504).

3.12 **Категорирование защищаемой информации**: Установление градаций важности защищаемой информации (СТ РК 34.026).

3.13 **Мероприятие по защите информации**: Совокупность действий, направленных на разработку и/или практическое применение способов и средств защиты информации (СТ РК 34.026).

3.14 **Непреднамеренное воздействие на информацию**: Ошибка пользователя информацией, сбой технических и программных средств информационных систем, природные явления или иные нецеленаправленные на изменение информации действия, приводящие к искажению, уничтожению, копированию, блокированию доступа к информации, а также к утрате, уничтожению или сбою функционирования носителя информации.

3.15 **Несанкционированное воздействие на информацию**: Воздействие на защищаемую информацию с нарушением установленных прав и/или правил доступа, приводящее к утечке, искажению, подделке, уничтожению, блокированию доступа к информации, а также к утрате, уничтожению или сбою функционирования носителя информации.

3.16 **Обработка информации**: Совокупность операций сбора, накопления, ввода, вывода, приема, передачи, записи, хранения, регистрации, уничтожения, преобразования, отображения, осуществляемых над информацией.

3.17 **Система защиты информации автоматизированной системы**: Совокупность технических, программных и программно-технических **средств защиты** информации и **средств контроля эффективности защиты** информации.

3.18 **Средство защиты информации**: Техническое, программное средство, вещество и/или материал, предназначенные или используемые для защиты информации (СТ РК 34.026).

3.19 **Средство контроля эффективности защиты информации:** Технические, программные и другие средства, предназначенные для контроля эффективности защиты информации, а также средства, в которых они реализованы. (СТ РК 34.026).

3.20 **Приемочный контроль**: Контроль продукции, по результатам которого принимается решение о ее пригодности к поставкам и/или использованию (ГОСТ 16504).

3.21 **Контроль эффективности защиты информации:** Проверка соответствия качественных и количественных показателей эффективности мероприятий по защите информации требованиям или нормам эффективности защиты информации (СТ РК 34.026).

3.22 **Специальная проверка**: Проверка компонентов автоматизированной системы, осуществляемая с целью поиска и изъятия закладного устройства.

3.23 **Специальные исследования (специсследования)**: Выявление с использованием контрольно-измерительной аппаратуры возможных технических каналов утечки защищаемой информации от основных и вспомогательных технических средств и

систем и оценка соответствия защиты информации требованиям нормативных документов по защите информации.

В настоящем стандарте приняты следующие сокращения:

АС - автоматизированная система;

АСЗИ - автоматизированная система в защищенном исполнении;

ЗИ - защита информации;

ТЗ - техническое задание;

ЧТЗ - частное техническое задание;

НД - нормативная документация;

ШС - шифровальное средство;

СиЗИ - система защиты информации;

СВТ - средство вычислительной техники;

ТС - технические средства;

ПС - программные средства;

СрЗИ - средство защиты информации;

НИР - научно-исследовательская работа;

ОКР - опытно-конструкторская работа;

НСД - несанкционированный доступ;

ПЭМИН - побочные электромагнитные излучения и наводки.

4 Общие положения

4.1 АС реализует информационную технологию в виде определенной последовательности информационно-связанных функций, задач или процедур, выполняемых в автоматизированном или автоматическом режимах.

4.2 Целесообразность создания и внедрения АС определяется социальным, научно-техническим или другими полезными эффектами, получаемыми в результате автоматизации.

4.3 Процесс создания АСЗИ заключается в выполнении совокупности мероприятий, направленных на разработку и/или практической применение информационной технологии, реализующей функции по ЗИ, установленные в соответствии с требованиями стандартов и/или нормативных документов по ЗИ как во вновь создаваемых, так и в действующих АС.

4.4 Целью создания АСЗИ является исключение или существенное затруднение получения злоумышленником защищаемой информации, обрабатываемой в АС, а также исключение или существенное затруднение несанкционированного и/или непреднамеренного воздействия на защищаемую обрабатываемую информацию и ее носители.

4.5 Защита информации в АСЗИ является составной частью работ по их созданию, эксплуатации и осуществляется во всех органах государственной власти и на предприятиях (организациях), располагающих секретной информацией [5].

4.6 Разработка и внедрение вновь создаваемой АС производится в соответствии с ТЗ. ТЗ на АС является основным документом, определяющим требования, предъявляемые к АС, порядок создания АС и приемку АС при вводе в эксплуатацию.

4.7 Для вновь создаваемых АС ТЗ разрабатывают на систему в целом, предназначенную для работы самостоятельно или в составе другой системы. Дополнительно могут быть разработаны ЧТЗ на части АС, на подсистемы АС. Поэтому требования по ЗИ при создании АСЗИ должны включаться разделом в общее ТЗ на АС или могут быть изложены в виде частного ЧТЗ или дополнения к основному ТЗ на АС.

Порядок утверждения и согласования ЧТЗ (дополнения к основному ТЗ на АС) не должен отличаться от установленного порядка утверждения и согласования ТЗ на АС по СТ РК 34.015.

4.8 Для АСЗИ, создаваемой на базе действующей АС, разрабатывается ТЗ (ЧТЗ) или дополнение к основному ТЗ на АС, в которые включаются требования по ЗИ только в части создаваемой системы (подсистемы) защиты обрабатываемой информации в АС.

Утверждение и согласование ТЗ (ЧТЗ) или дополнения к основному ТЗ на АС производится в порядке, установленном СТ РК 34.015.

4.9 Реализация мероприятий по защите информации в АСЗИ должна осуществляться непрерывно на всех стадиях и этапах создания АСЗИ во взаимосвязи с мерами по обеспечению установленного режима секретности проводимых работ.

Основные принципы и положения по созданию и функционированию АСЗИ должны соответствовать требованиям СТ РК ГОСТ Р 50739, СТ РК 1170, СТ РК ГОСТ Р 51275, [6].

Для **АСЗИ,** предназначенных для обработки **информации, составляющей государственные секреты**, а также несекретной информации с ограниченным доступом, используемой в управлении экологически опасными объектами, **требования вышеперечисленных документов являются обязательными.**

В остальных случаях требования вышеперечисленных документов несут рекомендательный характер и конкретные требования по созданию и функционированию АСЗИ в области защиты информации могут устанавливаться в нормативных документах, разрабатываемых собственником информации.

4.10 Типовое содержание работ на всех стадиях и этапах создания АСЗИ должно соответствовать требованиям ГОСТ 34.601, [7] и рекомендациям, приведенным в Приложении А.

4.11 Организации-участники работ по созданию АСЗИ должны иметь лицензии на право проведения работ в области защиты информации. Лицензирование организаций и предприятий осуществляется в установленном порядке.

4.12 Работы по созданию, производству и эксплуатации АСЗИ с использованием шифровальных средств для защиты секретной информации, организуются в соответствии с положениями нормативных актов Республики Казахстан, определяющих порядок разработки, изготовления и обеспечения эксплуатации шифровальных средств, систем и комплексов вооружения, использующих шифровальные средства.

4.13 Научно-техническое обеспечение создания АСЗИ должно соответствовать современному состоянию развития науки и техники, а технические решения по защите информации должны быть экономически оправданными.

4.14 Для создания АСЗИ могут применяться как серийно выпускаемые, так и вновь разработанные ТС и ПС обработки информации, а также технические, программные, программно-технические, шифровальные СрЗИ и средства для контроля эффективности. Выпускаемые средства должны иметь сертификаты соответствия, полученные в соответствии с [8] и правилами государственной системы технического регулирования Республики Казахстан.

Вновь разработанные средства должны быть сертифицированы в установленном порядке до начала опытной эксплуатации АСЗИ.

4.15 Процесс создания и применения АСЗИ должен быть документирован в полном соответствии с требованиями ГОСТ 34.201, в том числе и НД по защите обрабатываемой информации.

4.16 Заказчик, собственник и владелец АСЗИ, а также организации-участники создания АСЗИ несут ответственность за обеспечение зашиты обрабатываемой

информации в АСЗИ и выполняемые работы по ЗИ на всех стадиях создания АСЗИ как это предусмотрено в законодательстве Республики Казахстан.

4.17 Технические, программные и программно-технические СрЗИ специального применения создаются разработчиком АСЗИ. Конструкторская документация на их изготовление включается в состав документации на АСЗИ отдельными документами или разделами основных документов.

4.18 За обеспечение создания АСЗИ несут ответственность:

- **заказчик** - в части включения в ТЗ (ЧТЗ) на АСЗИ и ее компонентов, а также в техническую, программную, конструкторскую и эксплуатационную документацию обоснованных требований по защите обрабатываемой информации и контроля их выполнения в процессе экспертизы документации, испытаний и приемки как АСЗИ в целом, так и ее компонентов;

- **предприятие - разработчик** - в части обеспечения соответствия разрабатываемой АСЗИ и СиЗИ требованиям ТЗ (ЧТЗ) по защите обрабатываемой информации, действующим стандартам, нормам и другим НД;

- **предприятие - изготовитель** - в части осуществления технических мер по обеспечению соответствия изготавливаемых технических средств и программной продукции заданным требованиям по защите обрабатываемой информации, реализованным в конструкторской и программной документации.

4.19 Общее руководство работами по ЗИ при создании АСЗИ в целом осуществляет главный конструктор АСЗИ или его заместители, а при создании компонентов АСЗИ - главные конструктора этих компонентов или их заместители.

Методическое руководство работами по ЗИ в АСЗИ в процессе жизненного цикла АСЗИ осуществляют подразделения организаций (штатные специалисты) по ЗИ, участвующие в создании АСЗИ.

5 Особенности испытаний и применения автоматизированной системы в защищенном исполнении

5.1 Состав реализуемых стадий и этапов создания для каждой конкретной АСЗИ, а также содержание выполняемых на них работ по защите обрабатываемой информации устанавливают на стадии "Техническое задание" при разработке ТЗ (ЧТЗ) в соответствии с требованиями СТ РК 34.015.

Номенклатура требований по ЗИ, предъявляемая к АСЗИ, разрабатывается в соответствии с требованиями НД по ЗИ, содержащими требования по проведению сертификации комплектующих изделий, по проведению специальных исследований и специальных проверок средств обработки информации как иностранного, так и совместного производства и по проведению аттестации АСЗИ по требованиям безопасности информации.

5.2 Ввод АСЗИ в эксплуатацию осуществляется только после выполнения всех мероприятий по ЗИ и проведения испытаний испытательным центром (лабораторией) на соответствие требованиям НД по защите информации.

5.3 Применение АСЗИ для обработки защищаемой информации разрешается только после подтверждения соответствия установленным требованиям информационной безопасности.

5.4 Эксплуатация АСЗИ должна осуществляться в полном соответствии с утвержденной организационно-распорядительной и эксплуатационной документацией на АСЗИ, оценка которой должна быть дана при испытаниях АСЗИ на соответствие требованиям НД по защите информации.

5.5 Должностные лица, обслуживающий персонал и пользователи (операторы) АСЗИ несут ответственность за несоблюдение ими установленного порядка работы по ЗИ и применения мер и средств защиты информации.

5.6 При выявлении нарушений требований ЗИ на АСЗИ установленным НД эксплуатация АСЗИ должна быть прекращена.

5.7 Прекращение эксплуатации АСЗИ возможно также по следующим основаниям:

- согласно принятому собственником (владельцем) АСЗИ решению и оформленному в установленном порядке;
- согласно принятому решению органа контроля из-за несоответствия требованиям НД по защите информации или по другим причинам, приводящим к утечке ЗИ или другим угрозам защищаемой информации;
- по решению суда.

5.8 Организационно-методическое руководство работами по созданию, изготовлению, обеспечению и эксплуатации средств криптографической ЗИ, сертификации этих средств, а также контроль за состоянием и развитием этого направления работ осуществляют ведомства, уполномоченные Правительством Республики Казахстан на проведение соответствующих работ.

5.9 Порядок обеспечения эксплуатации АСЗИ с использованием шифровальной техники для защиты секретной информации, регламентируется в [9].

5.10 Ответственность за надлежащее исполнение правил эксплуатации средств криптографической ЗИ (в том числе во время приемочных испытаний) возлагается на руководство организаций, эксплуатирующих данные средства.

5.11 Контроль за выполнением требований инструкций по эксплуатации средств криптографической ЗИ возлагается на специальные подразделения по ЗИ на предприятии (организации) [9].

5.12 Тематические исследования по криптографической ЗИ в составе комплексов технических средств АСЗИ проводятся организациями, имеющими лицензию на этот вид работ в соответствии с [9].

5.13 Специальные исследования ТС и средств АСЗИ проводятся организациями (учреждениями), имеющими лицензии уполномоченного государственного органа на соответствующий вид деятельности.

5.14 Подтверждение соответствия требованиям информационной безопасности средств, комплексов и систем ЗИ осуществляется в соответствии с требованиями [8].

5.15 Аттестацию на соответствие требованиям защиты информации АСЗИ осуществляют в соответствии с требованиями действующих нормативных документов.

5.16 Испытания СВТ АСЗИ на соответствие требованиям по защите обрабатываемой информации от утечки за счет побочных электромагнитных излучений и наводок осуществляют в соответствии с требованиями действующих нормативных документов.

5.17 Испытания СВТ и АСЗИ на соответствие требованиям СТ РК ГОСТ Р 50739 по защите от НСД к информации осуществляют в соответствии с действующими нормативными документами.

5.18 Испытания программных средств АСЗИ на наличие компьютерных вирусов осуществляют в соответствии с требованиями действующих нормативных документов.

Приложение А
(рекомендуемое)

Типовое содержание работ на стадиях создания автоматизированных систем в защищенном исполнении

Таблица А.1

По ГОСТ 34.601		Типовое содержание работ по защите информации
Стадия	**Этапы работы**	
1 Формирование требований к АС	1.1 Обследование объекта и обоснование необходимости создания АСЗИ	Сбор данных о проводимых работах на объекте информатизации по обработке информации различной степени секретности. Определение факторов, воздействующих на информацию в соответствии с требованиями СТ РК ГОСТ Р 51275. Оценка целесообразности создания АСЗИ.
	1.2 Формирование требований пользователя к АСЗИ	Подготовка исходных данных для формирования требований по ЗИ на АС и процессов ее создания и эксплуатации. Разработка предварительных требований к СиЗИ на АСЗИ.
	1.3 Оформление отчета о выполняемой работе и заявки на разработку АСЗИ	Разработка предложений по ЗИ в отчетной нормативной и технической документации. Оформление отчета о выполненных работах по ЗИ на данных стадиях. Оформление предложений по ЗИ в заявку на разработку АСЗИ. Формирование предложений по ЗИ в ТЗ на АСЗИ.
2 Разработка концепции АС	2.1 Изучение объекта	Уточнение условий эксплуатации АСЗИ и категорий важности обрабатываемой информации. Формирование перечня угроз защищаемой информации. Уточнение номенклатуры требований, предъявляемых к АСЗИ.
	2.2 Проведение необходимых НИР	Поиск путей реализации требований по ЗИ в АС. Оценка возможности реализации требований по ЗИ в АСЗИ. Оформление и утверждение отчета о НИР по ЗИ или разделов по ЗИ в отчет о НИР по созданию АСЗИ.
	2.3 Разработка вариантов концепции АС и выбор варианта концепции АС	Разработка альтернативных вариантов концепции ЗИ в АС и облика СиЗИ и процессов ее создания. Выбор оптимального варианта концепции ЗИ в АС (разработка замысла ЗИ в АС) и СиЗИ АС. Технико-экономическое обоснование выбранного варианта ЗИ в АС и процессов ее создания и эксплуатации.
	2.4 Оформление отчета о выполненной работе	Подготовка и оформление отчета о выполненных работах по ЗИ на данной стадии создания АС. Согласование концепции ЗИ в АС и предложений по вариантам СиЗИ в АС. Предложения по ЗИ в отчетную нормативную и техническую документацию этапа работ. Согласование и получение заключения в уполномоченном государственном органе на разработку шифровальных средств.
3 Техническое задание	3.1 Разработка и утверждение технического задания на создание АСЗИ	Разработка требований по ЗИ в раздел ТЗ (ЧТЗ) на создание АСЗИ. Разработка, оформление, согласование и утверждение ТЗ (ЧТЗ) на создание АСЗИ.

Продолжение таблицы А.1

По ГОСТ 34.601		Типовое содержание работ по защите информации
Стадия	**Этапы работы**	
4 Эскизный проект	4.1 Разработка предварительных проектных решений по системе в целом и ее частям	Разработка предварительных проектных решений АСЗИ. Технико-экономическое обоснование эффективности вариантов СиЗИ. Разработка ТЗ на СрЗИ и средства контроля эффективности ЗИ. Разработка требований на СрЗИ и средства контроля эффективности ЗИ в АС.
	4.2 Разработка документации на АСЗИ и ее части	Разработка, оформление, согласование и утверждение документации по ЗИ и разделов эскизного проекта АС в части ЗИ. Экспертиза документации отчетной научно-технической документации и технической документации.
5 Технический проект	5.1 Разработка проектных решений по системе в целом и ее частям	Разработка СрЗИ н средств контроля. Разработка технического проекта СиЗИ и предложений по ЗИ в технический проект АСЗИ.
	5.2 Разработка документации на АСЗИ и ее части	Разработка рабочей документации и технического проекта СиЗИ АС. Разработка разделов технической документации по ЗИ и/или отдельных документов по ЗИ в АС. Участие в экспертизе документации АСЗИ.
	5.3 Разработка и оформление документации на поставку изделий для комплектования АСЗИ	Подготовка и оформление технической документации на поставку ТС и ПС для АС и СиЗИ. Поставка СрЗИ. Испытания СрЗИ. Сертификация СрЗИ и СиЗИ на соответствие требованиям по безопасности информации. Специсследования (спецпроверки) приобретенных ТС. Тестирование ПС. Экспертиза.
	5.4 Разработка заданий на проектирование в смежных частях проекта объекта автоматизации	Проектирование помещений АС с учетом требований НД по защите информации.
6 Рабочая документация	6.1 Разработка рабочей документации на систему в целом и ее части	Участие в разработке рабочей конструкторской документации АС в части учета требований по ЗИ. Разработка рабочей конструкторской документации СиЗИ. Участие в экспертизе рабочей конструкторской документации.
	6.2 Разработка или адаптация программ	Разработка ПС АСЗИ, программных СрЗИ. Тестирование ПС. Сертификация ПС по требованиям безопасности информации.

Окончание таблицы А.1

По ГОСТ 34.601		Типовое содержание работ по защите информации
Стадия	**Этапы работы**	
7 Ввод в действие	7.1 Подготовка АСЗИ к вводу в действие	Реализация проектных решений по организационной структуре СиЗИ АС и процесса. Требования к организационным мерам ЗИ
	7.2 Подготовка персонала	Проверка способности персонала обеспечить функционирование АСЗИ н СиЗИ. Проверка специалистов службы безопасности АС по обслуживанию СиЗИ.
	7.3 Комплектация АС поставляемыми изделиями (ПС и ТС)	Получение комплектующих изделий для СиЗИ. Проверка качества поставляемых комплектующих изделий
	7.4 Строительно-монтажные работы	Участие в работах по контролю за выполнением требований по ЗИ строительными организациями. Участие в испытаниях ТС по вопросам ЗИ. Проведение специсследований ТС
	7.5 Пуско-наладочные работы	Проведение автономных наладок технических и программных СрЗИ, загрузка информации в базу данных и ее проверка. Участие в комплексной наладке всех средств АС с точки зрения обеспечения ЗИ
	7.6 Проведение предварительных испытаний	Испытание СиЗИ на соответствие требованиям. Устранение недостатков СрЗИ и СиЗИ. Внесение изменений в документацию на СиЗИ. Участие в испытаниях АСЗИ. Проведение специсследований ТС. Аттестация АСЗИ
	7.7 Проведение опытной эксплуатации	Эксплуатация СиЗИ. Анализ, доработка, наладка СиЗИ. Акт о завершении опытной эксплуатации СиЗИ. Участие в опытной эксплуатации АСЗИ. Анализ и предложения по доработке АСЗИ.
8 Сопровождение АСЗИ	8.1 Выполнение работ в соответствии с гарантийными обязательствами	Устранение недостатков по ЗИ в процессе функционирования АСЗИ. Внесение изменений в документацию АС в части вопросов ЗИ. Проведение инспекционного контроля за стабильностью характеристик АСЗИ.
	8.2. Послегарантийное обслуживание	Анализ функционирования СиЗИ в АСЗИ. Установление причин не выполнения требований по ЗИ в АСЗИ. Выявление недостатков. Устранение недостатков в СиЗИ АСЗИ по гарантийным обязательствам. Внесение изменений в документацию на АСЗИ. Контроль состояния ЗИ в АС в защищенном исполнении.

Приложение
(справочное)

Библиография

[1] Закон Республики Казахстан	«О государственных секретах»
[2]	Концепция информационной безопасности Республики Казахстан
[3]	Соглашение между Правительством Республики Казахстан и Правительством Российской Федерации о сотрудничестве в области защиты информации
[4] Закон Республики Казахстан	«Об информатизации»
[5]	Постановление КМ РК №1111-43с 05.11.94 «Об утверждении Положения о государственной системе защиты информации РК».
[6] РД 50-680-88	Методические указания. Автоматизированные системы. Основные положения
[7] РД 50-34.698-90	Методические указания. Информационная технология. Комплекс стандартов и руководящих документов на автоматизированные системы. Автоматизированные системы. Требования к содержанию документов.
[8]	Постановление Правительства Республики Казахстан от 19 октября 2000 года N 1561 Об утверждении Правил выдачи сертификата соответствия технических средств защиты сведений, составляющих государственные секреты
[9]	Постановление Правительства РК от 13.06 97 № 967 «Об утверждении Положения о порядке лицензирования деятельности в области разработки, производства, ремонта и реализации криптографических средств защиты информации, специальных технических средств для проведения специальных оперативно-розыскных мероприятий и об утверждении квалификационных требований в Республике Казахстан

УДК 681.3 **МКС 35.040**

Ключевые слова: защищаемая информация, автоматизированная система, автоматизированная система в защищенном исполнении, требования по защите информации, средства защиты информации, средства контроля эффективности защиты информации, система защиты информации, аттестация автоматизированной системы в защищенном исполнении, сертификация средств защиты информации, лицензирование в области защиты информации, контроль эффективности защиты информации

Басуға _____ж. қол қойылды Пішімі 60х84 1/16
Қағазы офсеттік. Қаріп түрі «KZ Times New Roman»,
«Times New Roman»
Шартты баспа табағы 1,86. Таралымы ____ дана. Тапсырыс ____

«Қазақстан стандарттау және сертификаттау институты»
республикалық мемлекеттік кәсіпорны
010000, Астана қаласы, Есіл өзеннің жағалауы, № 35 көше, 11 үй,
«Эталон орталығы» ғимараты
Тел.: 8 (7172) 240074

ПОПРАВКИ, ПРИНЯТЫЕ К ГОСУДАРСТВЕННЫМ СТАНДАРТАМ РЕСПУБЛИКИ КАЗАХСТАН

Указатель нормативных документов по стандартизации.

В каком месте	Напечатано	Должно быть
Часть 2	СТ РК ИСО 1823-2006 (ИСО 1823-1-1997, IDT)	СТ РК ИСО 1823-1-2006 (ИСО 1823-1-1997 IDT)

(ИУС № 4 2007 г.)

Указатель нормативных документов по стандартизации.

В каком месте	Напечатано	Должно быть
Часть 6	1823-1-2005 ИСО 1823-1	1823-1-2006 ИСО1823-1

(ИУС № 4 2007 г.)

Указатель нормативных документов по стандартизации.

В каком месте	Напечатано	Должно быть
Часть 6 СТ РК 34.025-2006	Код МКС 01.040.01	Код МКС 35.040

(ИУС № 4 2007 г.)

Указатель нормативных документов по стандартизации.

В каком месте	Напечатано	Должно быть
Часть 6 СТ РК 34.025-2006	№ 536 от 11.12.2006 г	№ 550 от 15.12.2006

(ИУС № 4 2007 г.)