



ГОСУДАРСТВЕННЫЙ СТАНДАРТ РЕСПУБЛИКИ КАЗАХСТАН

СИСТЕМЫ КОНТРОЛЯ И УПРАВЛЕНИЯ ДОСТУПОМ

Общие технические требования

СТ РК 1699 - 2007

Издание официальное

**Комитет по техническому регулированию и метрологии
Министерства индустрии и торговли Республики Казахстан**

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 24 декабря 2007 г. № 691

3 В настоящем стандарте реализованы нормы законов Республики Казахстан О техническом регулировании от 09.11.2004 г № 603-ІІ., О национальной безопасности от 26.06.98 г. № 233-І, О государственных секретах от 15.03.99 г № 349-1., О борьбе с терроризмом от 13.07.99 г № 416-І., О языках в Республике Казахстан от 11.07.97 г №151-І

**4 СРОК ПЕРВОЙ ПРОВЕРКИ
ПЕРИОДИЧНОСТЬ ПРОВЕРКИ**

2012 год
5 лет

5 ВВЕДЕН ВПЕРВЫЕ

Информация об изменениях к настоящему стандарту публикуется в ежегодно издаваемом информационном указателе «Нормативные документы по стандартизации», а текст изменений и поправок — в ежемесячно издаваемых информационных указателях «Нормативные документы по стандартизации». В случае пересмотра (изменения, замены) или отмены настоящего стандарта соответствующая информация будет опубликована в ежемесячно издаваемом информационном указателе «Нормативные документы по стандартизации»

Содержание

1 Область применения	1
2 Нормативные ссылки	1
3 Термины и определения	2
4 Сокращения	3
5 Общие положения	3
6 Классификация СКУД	4
7 Технические требования к системам контроля и управления доступом	4
Приложение (справочное). Библиография	11

ГОСУДАРСТВЕННЫЙ СТАНДАРТ РЕСПУБЛИКИ КАЗАХСТАН

СИСТЕМЫ КОНТРОЛЯ И УПРАВЛЕНИЯ ДОСТУПОМ**Общие технические требования**

Дата введения 2009.01.01.

1 Область применения

Настоящий стандарт распространяется на технические системы контроля и управления санкционированным доступом и перемещением людей, транспорта и иных объектов в (из) контролируемые здания, помещения, специальные зоны и территории.

Стандарт устанавливает общие требования и классификацию систем контроля и управления доступом отечественного и иностранного производства.

Требования настоящего стандарта предназначены для применения органами государственной власти и управления, а также организациями и предприятиями, в которых обрабатывается информация, подлежащая защите в интересах национальной безопасности Республики Казахстан.

Стандарт пригоден для целей подтверждения соответствия.

2 Нормативные ссылки

В настоящем стандарте использованы ссылки на следующие стандарты:

СТ РК 34.005-2002 Информационная технология. Основные термины и определения.

СТ РК 1174-2003 Пожарная техника для защиты объектов. Основные виды. Размещение и обслуживание.

СТ РК 1201-2002 Порядок разработки, согласования, утверждения и государственной регистрации средств защиты информации.

СТ РК ИСО/МЭК 17799-2006. Информационная технология. Методы обеспечения защиты. Свод правил по управлению защитой информации.

СТ РК ГОСТ Р 50571.22-2006 Электроустановки зданий. Часть 7. Требования к специальным электроустановкам. Раздел 707. Заземление оборудования обработки информации.

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

ГОСТ 2.601-2006 Единая система конструкторской документации. Эксплуатационные документы.

ГОСТ 12.1.003-83 Система стандартов безопасности труда. Шум. Общие требования безопасности.

ГОСТ 12.1.004-91 Система стандартов безопасности труда. Пожарная безопасность. Общие требования.

ГОСТ 12.1.006-84 Система стандартов безопасности труда. Электромагнитные поля радиочастот. Допустимые уровни на рабочих местах и требования к проведению контроля.

ГОСТ 12.2.007.0-75 Система стандартов безопасности труда. Изделия электротехнические. Общие требования безопасности.

Издание официальное

ГОСТ 27.003-90 Надежность в технике. Состав и общие правила задания требований по надежности

ГОСТ 15150-69 Машины, приборы и другие технические изделия. Исполнения для различных климатических районов. Категории, условия эксплуатации, хранения и транспортирования в части воздействия климатических факторов внешней среды.

ГОСТ 28934-91 Совместимость технических средств электромагнитная. Содержание раздела технического задания в части электромагнитной совместимости.

ГОСТ Р ИСО/МЭК ТО 10178-98* Информационная технология. Передача данных и обмен информацией между системами. Структура и кодирование адресов управления логическим звеном в локальных вычислительных сетях.

ГОСТ Р 51318.22-99 (СИСПР 22-97)* Совместимость технических средств электромагнитная. Радиопомехи промышленные от оборудования информационных технологий. Нормы и методы испытаний.

Примечание — При пользовании настоящим стандартом целесообразно проверить действие ссылочных стандартов по указателю «Нормативные документы по стандартизации», составленному по состоянию на 1 января текущего года, и по соответствующим информационным указателям, опубликованным в текущем году. Если стандарт заменен (изменен), то при пользовании настоящим стандартом следует руководствоваться замененным (измененным) стандартом. Если стандарт отменен без замены, то положение, в котором дана ссылка на него, применяется в части, не затрагивающей эту ссылку.

3 Термины и определения

В настоящем стандарте применяются термины по СТ РК 34.005, а также следующие термины с соответствующими определениями:

3.1 Аутентификация: Проверка принадлежности субъекту доступа предъявленного им идентификатора и подтверждение его подлинности.

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

3.3 Зона доступа: Совокупность точек доступа, связанных общим местоположением или другими характеристиками.

3.4 Идентификация субъектов доступа: Присвоение субъектам доступа идентификаторов и (или) сравнение предъявляемых идентификаторов с перечнем присвоенных идентификаторов, владельцы (носители) которых допущены на объект.

3.5 Несанкционированный доступ: Получение защищаемой информации заинтересованным субъектом с нарушением установленных правовыми документами или собственником, владельцем информации прав или правил доступа к ней.

3.6 Правило двух (и более) лиц: Правило доступа, при котором доступ разрешен только при одновременном присутствии двух и более людей.

3.7 Разграничение доступа: Порядок доступа лиц к техническим и программным средствам, секретной информации при ее обработке на средствах вычислительной техники в соответствии с заранее разработанными и утвержденными правилами.

3.8 Релейный уровень интеграции: Уровень, который предполагает наличие дополнительного модуля в контроллере (или дополнительных входов/выходов в контроллере), к которым подключаются охранные или пожарные извещатели и релейные выходы для управления телекамерами и другими устройствами.

3.9 Система контроля и управления доступом: Совокупность средств (элементов) контроля и управления, обладающих технической, информационной,

* На территории Республики Казахстан стандарт применяется в соответствии с СТ РК 1.9

программной и эксплуатационной совместимостью.

3.10 Средства контроля и управления доступом: Механические, электромеханические, электрические, электронные устройства, конструкции и программные средства, обеспечивающие реализацию контроля и управления доступом.

3.11 Техническое задание: Исходный технический документ заказчика на выполнение опытно-конструкторской работы, устанавливающий комплекс требований к содержанию, объему и срокам выполнения работы по созданию (модернизации) изделия.

3.12 Точка доступа: Место, где непосредственно осуществляется контроль доступа, оборудованное необходимыми средствами аутентификации, идентификации и исполнительными механизмами (например, турникет, кабина прохода, дверь, шлагбаум).

3.13 Уровень доступа: Совокупность интервалов времени доступа и точек доступа, которые назначаются определенному лицу или группе лиц, имеющих доступ в заданные точки доступа в заданные интервалы времени.

4 Сокращения

В настоящем стандарте приняты следующие сокращения:

СКУД – система контроля и управления доступом;

ОКР - опытно-конструкторская работа;

ТЗ – техническое задание;

ЭВМ – электронно-вычислительная машина.

5 Общие положения

5.1 Система контроля и управления доступом должна соответствовать требованиям настоящего стандарта. Функциональные характеристики и параметры СКУД устанавливаются нормативными документами по стандартизации в зависимости от требований к системе.

5.2 Проектирование (модернизация) и внедрение СКУД проводится, как правило, в рамках ОКР. Функции основных участников ОКР, взаимоотношения между ними, правила выполнения и порядок реализации законченной ОКР определены СТ РК 1201.

5.3 Проектирование и внедрение вновь создаваемой (модернизируемой) СКУД производится в соответствии с ТЗ. ТЗ на СКУД является основным документом, определяющим требования, предъявляемые к системе, порядку её создания (модернизации) и приемки при вводе в эксплуатацию.

5.4 При построении СКУД на базе локальных вычислительных сетей и при интегрировании СКУД с другими системами на системном уровне (например, с охранной, пожарной сигнализацией, с системами видеоконтроля), структура и кодирование адресов управления для обмена информацией между системами должны соответствовать ГОСТ Р ИСО/МЭК ТО 10178.

Протоколы обмена информацией должны обеспечивать необходимую помехоустойчивость, как от промышленных, так и от преднамеренных помех, необходимую скорость обмена информацией и должны быть установлены в ТЗ и (или) в нормативных документах по стандартизации.

5.5 Организации – участники работ по созданию СКУД должны иметь лицензию на право проведения работ в области защиты информации. Лицензирование организаций осуществляется в установленном порядке [1].

5.6 В процессе проектирования (модернизации), монтажа и эксплуатации СКУД должна быть организована разрешительная система доступа разработчиков, специалистов

по монтажу и наладке, обслуживающего и эксплуатирующего персонала к техническим, программным и программно-техническим средствам СКУД, предотвращающих или существенно затрудняющих несанкционированный доступ к секретной информации государства и других собственников.

6 Классификация СКУД

Системы контроля и управления доступом классифицируются по:

- способу управления;
- количеству контролируемых точек доступа;
- функциональным характеристикам;
- виду объектов контроля;
- уровню защищенности объектов контроля от несанкционированного доступа.

6.1 По способу управления СКУД подразделяются на:

- автономные – для управления одним или несколькими устройствами, преграждающими доступ в точку доступа, без передачи информации из контролируемой точки доступа на центральный пульт и без контроля со стороны оператора;

- централизованные (сетевые) – для управления одним или несколькими устройствами, преграждающими доступ в контролируемые точки доступа, с обменом информацией точки доступа с центральным пультом, контролем и управлением системой со стороны оператора;

- универсальные – включающие функции как автономных, так и сетевых систем, работающие в сетевом режиме под управлением центрального устройства управления и переходящие в автономный режим при возникновении отказов в сетевом оборудовании, в центральном устройстве управления или обрыве связи.

6.2 По количеству контролируемых точек доступа СКУД подразделяются на:

- малой емкости (менее 16 точек);
- средней емкости (от 16 до 63 точек);
- большой емкости (64 точки и более).

6.3 По функциональным характеристикам СКУД подразделяются на три класса:

- 1 – системы с ограниченными функциями;
- 2 – системы с расширенными функциями;
- 3 – многофункциональные системы.

6.4 По виду объектов контроля СКУД подразделяются:

- для контроля доступа физических лиц, транспорта и иных объектов в контролируемые точки доступа;

- для контроля доступа к информации.

6.5 По уровню защищенности объектов контроля от несанкционированного доступа СКУД подразделяются на:

- нормальные;
- повышенной устойчивости;
- высокой устойчивости.

7 Технические требования к системам контроля и управления доступом

7.1 Требования к функциональным характеристикам

7.1.1 Общие функциональные характеристики СКУД

СКУД должны обеспечивать выполнение основных положений правил разграничения доступа, установленных СТ РК ИСО/МЭК 17799.

В общем случае в ТЗ (нормативных документах по стандартизации) для конкретной системы, независимо от способа управления, должны быть заданы следующие характеристики и требования:

- максимальное количество точек доступа, зон доступа, пользователей;
- максимальная пропускная способность системы в точках доступа;
- количество и временные интервалы (окна времени) доступа;
- количество уровней доступа по статусу идентифицированного субъекта;
- количество и тип устройств идентификации и аутентификации в системе;
- максимальное расстояние от наиболее удаленной точки доступа до устройств управления;
- максимальное время реакции на события в системе;
- время хранения информации о событиях в памяти системы;
- максимальное количество событий, хранимых в памяти системы;
- ведение журнала событий (даты и времени возникновения; субъекта, осуществляющего регистрируемое действие и тип события; результат реакции системы);
- вероятность несанкционированного доступа, вероятность ложного задержания.

7.1.2 Автономные системы

7.1.2.1 Автономные СКУД, дополнительно к 7.1.1, должны обеспечивать:

- открывание устройств, преграждающих доступ, при считывании зарегистрированного в памяти идентификационного признака;
- запрет открывания устройств, преграждающих доступ, при считывании незарегистрированного в памяти идентификационного признака;
- сохранение идентификационных признаков в памяти системы при отказе и отключении электропитания;
- ручное, полуавтоматическое или автоматическое открывание устройств, преграждающих доступ для прохода при аварийных ситуациях, пожаре, технических неисправностях системы в соответствии с правилами установленного режима и правилами противопожарной безопасности;
- автоматическое формирование сигнала сброса на устройствах, преграждающих доступ, при отсутствии факта прохода;
- выдачу сигнала тревоги при использовании системы аварийного открывания устройств, преграждающих доступ для несанкционированного проникновения.

7.1.2.2 Необходимые дополнительные характеристики автономных СКУД в зависимости от функциональных характеристик для соответствующих классов систем приведены в таблице 1.

Таблица 1 - Дополнительные характеристики автономных СКУД в зависимости от функциональных характеристик для соответствующих классов систем

Функциональные характеристики автономной системы	Класс системы		
	1	2	3
1 Установка уровней доступа	-	+/-	+
2 Установка интервалов времени доступа	-	+/-	+
3 Возможность установления времени открывания устройств, преграждающих доступ	-	+/-	+
4 Защита от повторного использования идентификатора для прохода в одном направлении	-	+/-	+
5 Ввод специального идентификационного признака для открывания под принуждением	-	+/-	+
6 Защита от использования идентификаторов, запрещенных в системе (утрачены, отменены или субъект уволен)	-	+/-	+
7 Защита от манипулирования с целью подбора кода или его изменения	-	+/-	+
8 Подключение различных типов устройств идентификации и аутентификации	-	+/-	+/-
9 Доступ по «правилу двух (и более) лиц»	-	+/-	+/-
10 Световая индикация о состоянии доступа	+/-	+	+
11 Контроль состояния устройств, преграждающих доступ	+/-	+	+
12 Световое и (или) звуковое оповещение о попытках НСД	+/-	+/-	+
13 Регистрация и хранение информации о событиях в энергонезависимой памяти	-	+	+
14 Количество событий, хранимых в энергонезависимой памяти, не менее	-	16	64
15 Регистрация даты и времени возникновения событий	-	+/-	+
16 Возможность подключения принтера для вывода информации	-	+/-	+
17 Возможность передачи информации на устройства сбора информации или ЭВМ	-	+/-	+
18 Возможность объединения в сеть и обмена информацией с устройствами сбора информации и управления (ЭВМ)	-	+/-	+
19 Возможность интегрирования с системой охранной и (или) пожарной сигнализации на релейном уровне	-	+/-	+
20 Возможность интегрирования с системой видеоконтроля на релейном уровне	-	+/-	+
21 Возможность подключения дополнительных средств специального контроля, средств досмотра	-	-	+/-
Примечание - Знак «+» означает наличие функции и обязательность ее проверки при установлении класса, знак «-» - отсутствие функции, знак «+/-» - наличие функции необязательно.			

7.1.3 Системы с централизованным управлением и универсальные системы

7.1.3.1 Системы с централизованным управлением и универсальные СКУД должны соответствовать требованиям 7.1.2 и дополнительно обеспечивать:

- регистрацию и протоколирование тревожных и текущих сообщений;
- приоритетное отображение тревожных событий;
- управление в точках доступа работой устройств, преграждающих доступ, по команде оператора;
- задание интервалов времени действия идентификаторов в точках доступа и уровней доступа;
- защиту технических и программных средств от несанкционированного доступа к элементам управления, установки режимов и к информации;
- автоматический контроль исправности средств, входящих в систему, и линий передачи информации;
- возможность автономной работы контроллеров системы с сохранением контроллерами основных функций при отказе связи с пунктом централизованного управления;
- установку режимов свободного доступа с пункта управления при аварийных ситуациях и чрезвычайных происшествиях (пожар, землетрясение, взрыв и т. п.);
- блокировку прохода по точкам доступа командой с пункта управления в случае нападения;
- возможность подключения дополнительных средств специального контроля, средств досмотра.

7.1.3.2 Универсальные системы должны обеспечивать автономную работу при возникновении отказов в сетевом оборудовании, в центральном устройстве или обрыве связи, а также восстановление режимов работы после устранения отказов и восстановления связи.

7.1.3.3 Необходимые дополнительные характеристики СКУД с централизованным управлением и универсальных систем в зависимости от функциональных характеристик для соответствующих классов систем приведены в таблице 2.

Таблица 2 - Дополнительные характеристики СКУД с централизованным управлением и универсальных систем в зависимости от функциональных характеристик для соответствующих классов систем

Функциональные характеристики систем с централизованным управлением и универсальных систем	Класс системы		
	1	2	3
1 Количество уровней доступа	2	8	16
2 Количество интервалов времени доступа	2	8	16
3 Защита от повторного использования идентификатора для прохода в одном направлении	+/-	+	+
4 Ввод специального идентификационного признака для открывания под принуждением	+/-	+/-	+
5 Защита от использования идентификаторов, запрещенных в системе (утрачены, отменены или субъект уволен)	+/-	+/-	+
6 Защита от манипулирования с целью подбора кода или его изменения	+/-	+/-	+
7 Подключение различных типов устройств идентификации и аутентификации	+/-	+	+
8 Доступ по «правилу двух (и более) лиц»	+/-	+/-	+/-

Окончание таблицы 2

Функциональные характеристики систем с централизованным управлением и универсальных	Класс системы		
	1	2	3
9 Количество событий, сохраняемых в энергонезависимой памяти контроллеров, не менее	50	250	1000
10 Возможность интегрирования с системой охранной и (или) пожарной сигнализации на релейном уровне	+/-	+/-	+/-
11 Возможность интегрирования с системой видеоконтроля на релейном уровне	+/-	+/-	+/-
12 Возможность интегрирования с системой охранной, пожарной сигнализации и системами видеоконтроля на системном уровне	+/-	+/-	+
13 Возможность управления работой дополнительных устройств в точках доступа (освещение, вентиляция, лифты, технологическое оборудование и т. п.)	-	+/-	+/-
14 Возможность подключения переговорных устройств и (или) средств связи в точках доступа	-	+/-	+/-
15 Обеспечение изображения на экране ЭВМ плана объекта и (или) помещений объекта с указанием мест расположения средств контроля доступа, охранной и пожарной сигнализации, средств видеоконтроля и графическим отображением тревожных состояний в контрольных точках	+/-	+/-	+
16 Интерактивное управление средствами по изображению плана объекта на экране ЭВМ	-	-	+/-
17 Ведение баз данных на сотрудников (пользователей)	+/-	+	+
18 Поддержание фотографических данных пользователей в базе данных	-	+/-	+
19 Контроль за перемещением и поиск сотрудников	+/-	+/-	+
20 Контроль времени нахождения на объекте посетителей	+/-	+/-	+
Примечание - Знак «+» означает наличие функции и обязательность ее проверки при установлении класса, знак «-» - отсутствие функции, знак «+/-» - наличие функции необязательно.			

7.1.3.4 Программное обеспечение СКУД должно быть защищено от несанкционированного доступа. Требования разграничения доступа к программному обеспечению системы устанавливаются по СТ РК ГОСТ Р 50739.

7.2 Требования электромагнитной совместимости

Перечень показателей электромагнитной совместимости элементов СКУД должен соответствовать ГОСТ 28934.

Уровень допустимых радиопомех, создающихся при работе СКУД, не должен превышать норм, установленных ГОСТ Р 51318.22.

7.3 Требования к электропитанию

7.3.1 Электропитание элементов (средств контроля и управления) СКУД в зависимости от их назначения, должно осуществляться от следующих источников тока:

- сети переменного тока с номинальным напряжением 220 В и номинальной частотой 50 Гц;
- внешнего источника постоянного тока с номинальным напряжением 12 или 24 В;
- собственных источников тока напряжением, определяемым типом примененных аккумуляторов, сухих элементов или других источников тока.

СКУД должна сохранять свои функциональные характеристики и параметры, указанные в ТЗ или в нормативных документах по стандартизации, при изменении напряжения питания её элементов (средств контроля и управления) относительно номинального в пределах:

- от минус 15 % до плюс 10 % - для элементов с питанием от сети переменного тока;
- от минус 10 % до плюс 30 % - для элементов с питанием от аккумуляторов, в зависимости от предусмотренного назначения.

В элементах СКУД, питание которых осуществляется от источников постоянного тока, должна быть предусмотрена защита от повреждения при неправильном включении полярности электропитания.

7.3.2 Элементы СКУД должны иметь резервное электропитание в случае пропадания напряжения основного источника, при этом переход на резервный источник питания должен производиться автоматически, без нарушения заданных режимов работы и функциональных характеристик системы. Время перехода на резервный источник питания и время работы от него должны быть заданы в ТЗ и (или) в нормативных документах по стандартизации.

7.3.3 Допускается не применять резервный источник питания для исполнительных элементов системы, имеющих значительное энергопотребление. Такие исполнительные элементы при пропадании напряжения питания должны обеспечивать прекращение доступа и блокироваться в этом состоянии, для разблокировки они должны быть оборудованы аварийными механизмами открывания.

7.4 Требования безопасности

7.4.1 При монтаже, эксплуатации и проведении измерений параметров и тестировании СКУД должны выполняться требования ГОСТ 12.1.030, ГОСТ 12.2.007.0, [2], а также требования безопасности, изложенные в инструкциях по эксплуатации элементов и средств СКУД, контрольно - измерительных приборов.

7.4.1.1 В СКУД должна быть предусмотрена защита обслуживающего персонала от поражения электрическим током в процессе изготовления, монтажа, эксплуатации и технического обслуживания.

7.4.1.2 В СКУД должна быть исключена возможность воспламенения аппаратуры при случайном замыкании в цепях питания, при неправильном включении полярности электропитания, при коротком замыкании выхода излучающей аппаратуры, а также в условиях неисправностей.

7.4.1.3 Применение средств защиты, снижающих вероятность возникновения пожара, должно соответствовать нормативам по СТ РК 1174 и ГОСТ 12.1.004.

Температура наружных поверхностей аппаратуры во время работы при нормальных климатических условиях не должна превышать 318 °К (45 °С) в местах постоянного контакта оператора с поверхностью и 333 °К (60 °С) - в местах случайного прикасания к

поверхности.

7.4.2 Заземление средств контроля и управления, элементов СКУД должно соответствовать СТ РК ГОСТ Р 50571.22.

Элементы заземления должны быть расположены в местах, обеспечивающих удобство контроля переходного сопротивления.

7.4.3 Значение сопротивления изоляции электрических цепей аппаратуры СКУД и электрическая прочность изоляции должны быть заданы в ТЗ (нормативных документах по стандартизации).

7.4.4 По уровню шума, создаваемого в помещениях и на рабочих местах, элементы СКУД должны соответствовать ГОСТ 12.1.003.

СКУД должна соответствовать ГОСТ 12.1.006 по требованиям к допустимым уровням создаваемых электромагнитных полей радиочастот на рабочих местах персонала.

7.5 Требования по устойчивости к климатическим воздействиям

В процессе эксплуатации СКУД должна сохранять свои функциональные характеристики и параметры, указанные в ТЗ и (или) нормативных документах по стандартизации, при климатических воздействиях установленных ГОСТ 15150.

7.6 Требования к эксплуатационной документации

Общие требования к эксплуатационной документации по ГОСТ 2.601 и СТ РК ГОСТ Р 50739.

Номенклатура эксплуатационных документов устанавливаются по согласованию между заказчиком (потребителем) и разработчиком (изготовителем).

7.7 Требования к надежности

Показатели надежности СКУД задаются в ТЗ и нормативных документах по стандартизации в соответствии с требованиями, установленными ГОСТ 27.003.

Номенклатура показателей надежности и их предельно допустимые значения устанавливаются по согласованию между заказчиком (потребителем) и разработчиком (изготовителем).

7.8 Гарантийные обязательства

Гарантийные обязательства должны быть установлены в нормативных документах по стандартизации на СКУД или в договоре на поставку.

Показатели гарантийных обязательств должны определять:

- гарантийный срок хранения в календарном исчислении;
- гарантийный срок эксплуатации в календарном исчислении;
- гарантийную наработку в численных значениях ресурса (в часах работы).

Начальный момент исчисления гарантийных сроков и конкретные значения перечисленных видов гарантийных обязательств устанавливаются по согласованию между заказчиком (потребителем) и разработчиком (изготовителем).

Приложение
(справочное)

Библиография

[1] Правила лицензирования деятельности по технической защите государственных секретов Республики Казахстан, утверждены Постановлением Правительства Республики Казахстан от 14.12.2000г № 1842.

[2] Правила техники безопасности при эксплуатации электроустановок потребителей, утвержденные 21.12.84 г. Главгосэнергонадзором.

УДК 001.4:025.4.006.354

МКС 35.080

Ключевые слова: доступ, уровень доступа, несанкционированный доступ, система, информация, идентификация.

Басуға _____ ж. қол қойылды Пішімі 60x84 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 өзенінің сол жақ жағалауы, Орынбор көшесі, 11 үй,
«Эталон орталығы» ғимараты
Тел.: 8 (7172) 240074