ОСТ 95 10537-97

Группа Ф71

СТАНДАРТ ОТРАСЛИ

ОСНАЩЕНИЕ ПРОГРАММНО-АППАРАТНОЕ СИСТЕМ УЧЕТА И КОНТРОЛЯ ЯДЕРНЫХ МАТЕРИАЛОВ

Общие требования

ОКС 27.120.30
ОКСТУ 0024

Дата введения 1997-12-01

Предисловие

1 РАЗРАБОТАН Российским Федеральным Ядерным центром - Всероссийским научно-исследовательским институтом экспериментальной физики (РФЯЦ-ВНИИЭФ)

2 УТВЕРЖДЕН И ВВЕДЕН В ДЕЙСТВИЕ руководством Минатома России приказом от 07.10.1997 г. N 643

3 СОГЛАСОВАН Департаментом защиты информации, ядерных материалов и объектов Минатома России

4 ВВЕДЕН ВПЕРВЫЕ

5 ЗАРЕГИСТРИРОВАН Центральным научно-исследовательским институтом управления экономики и информации (ЦНИИАтоминформ) за ВР N 4044

6 ОТВЕТСТВЕННЫЙ ЗА ПРОВЕРКУ СТАНДАРТА - РФЯЦ-ВНИИЭФ

7 ДЕРЖАТЕЛЬ ПОДЛИННИКА СТАНДАРТА - Научно-конструкторское бюро по стандартизации и сертификации (НКБС)

8 ПЕРЕИЗДАНИЕ. Февраль 2003 г.

1 Область применения

Настоящий стандарт устанавливает общие требования к программно-аппаратным составляющим автоматизированной системы учета и контроля ядерных материалов на предприятиях, ядерных установках Министерства Российской Федерации по атомной энергии.

Настоящий стандарт является обязательным для предприятий ДЗИЯМО, ДЯТЦ, ДР ЯБП, ДП ЯБП, ДАЭ, ДАНТ, акционерного общества "Концерн "ТВЭЛ", государственного концерна "Росэнергоатом", всерегионального объединения "Изотоп", внешнеторгового объединения Техснабэкспорт.

2 Нормативные ссылки

В настоящем стандарте использованы ссылки на следующие стандарты:

ГОСТ 12.1.004-91 ССБТ. Пожарная безопасность. Общие требования

ГОСТ 12.4.009-83 ССБТ. Пожарная техника для защиты объектов. Основные виды. Размещение и обслуживание

ГОСТ 19.001-77 ЕСПД. Общие положения

ГОСТ 19.101-77 ЕСПД. Виды программ и программных документов

ГОСТ 19.102-77 ЕСПД. Стадии разработки

ГОСТ 19.103-77 ЕСПД. Обозначение программ и программных документов

ГОСТ 24.104-85 Единая система стандартов автоматизированных систем управления. Автоматизированные системы управления. Общие требования

ГОСТ 34.003-90 Информационная технология. Комплекс стандартов на автоматизированные системы. Автоматизированные системы. Термины и определения

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

ГОСТ 34.401-90 Информационная технология. Комплекс стандартов на автоматизированные системы. Средства технические периферийные автоматизированных систем дорожного движения. Типы и технические требования

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

ГОСТ 34.602-89 Информационная технология. Комплекс стандартов на автоматизированные системы. Техническое задание на создание автоматизированной системы

ГОСТ 34.603-92 Информационная технология. Виды испытаний автоматизированных систем

ГОСТ 16325-88 Машины вычислительные электронные цифровые общего назначения. Общие технические требования

ГОСТ 27201-87 Машины вычислительные электронные персональные. Типы, основные параметры, общие технические требования

ГОСТ 28147-89 Системы обработки информации. Защита криптографическая. Алгоритмы криптографического преобразования

ГОСТ Р 34.10-94* Информационная технология. Криптографическая защита информации. Процедуры выработки и проверки электронной цифровой подписи на базе асимметричного криптографического алгоритма

_____

* На территории Российской Федерации действует ГОСТ Р 34.10-2001. Здесь и далее. - Примечание изготовителя базы данных.

ГОСТ Р 34.11-94 Информационная технология. Криптографическая защита информации. Функция хэширования

Р 50-34.119-90 Рекомендации. Информационная технология. Комплекс стандартов на автоматизированные системы. Архитектура локальных вычислительных сетей в системах промышленной автоматизации. Общие положения

РД 50-34.698-90 Методические указания. Информационная технология. Комплекс стандартов и руководящих документов на автоматизированные системы. Автоматизированные системы. Требования к содержанию документов

РД 50-680-88 Методические указания. Автоматизированные системы. Основные положения

3 Определения и сокращения

В настоящем стандарте применяют следующие сокращения и термины с соответствующими определениями.

3.1 **Оснащение программно-аппаратное** - совокупность средств программной поддержки и средств вычислительной техники (компьютерное оборудование и сети) автоматизированной системы учета и контроля (АСУиК) ядерных материалов.

3.2 **Ядерный материал в документах по учету и контролю (ЯМ)** - ядерный и специальный неядерный материал, подлежащий учету и контролю в соответствии с перечнем, прилагаемым к концепции [1].

3.3 **СУиК** - программно-аппаратная составляющая автоматизированной системы учета и контроля ЯМ на предприятии.

3.4 **Зона баланса материалов (ЗБМ)** - территориально и административно установленная в пределах ядерной установки или пункта хранения ЯМ зона для учета и контроля ЯМ, в которой на основании измерений определено количество ЯМ при каждом их перемещении в зону и из нее и подведен баланс ЯМ за установленный период времени.

3.5 **Ключевая точка измерения** - место в ЗБМ, в котором ЯМ находятся в такой форме, что они могут быть измерены для определения потока материалов или их инвентарного количества.

3.6 **Информационная подсистема** - совокупность программных средств и данных, обеспечивающих на предприятии информационное сопровождение системы учета и контроля ЯМ.

3.7 **Информационный центр** - центр сбора и обработки информации по учету и контролю ЯМ в Минатоме России.

3.8 **Паспортные данные ЯМ** - исходные данные на ЯМ, хранящиеся в системе учета и контроля.

3.9 **Специальный отчет** - отчет, представляемый предприятием в вышестоящие организации в связи с потерей, несанкционированным использованием и хищением ЯМ, а также предполагаемой утратой ЯМ при чрезвычайном происшествии на ядерной установке.

3.10 **Контур обслуживания пользователя** - совокупность программно-аппаратных средств, задействованных в решении задач данного пользователя.

3.11 **ЭВТ** - электронно-вычислительная техника.

4 Назначение СУиК

4.1 С точки зрения учета, контроля и сохранности ЯМ предприятие представляет собой совокупность зон (одну зону) баланса материалов. В каждой зоне баланса на основании величин, измеренных в ключевых точках измерений, нормативных или паспортных данных (если измерение невозможно или нецелесообразно на предприятии) определяется количество ЯМ при каждом перемещении их в зону, или из нее, или в пределах зоны. Соответственно, в каждой зоне может быть подведен баланс ЯМ за установленный период времени, а по совокупности всех зон - баланс по предприятию в целом в соответствии с концепцией [1].

4.2 В настоящем стандарте сформулированы общие требования к автоматизированной системе, в которой едино и неразрывно осуществляется проводимый в настоящее время учет ЯМ, фиксируемый на бумажных носителях (журналах, накладных и т.п.) и на магнитных носителях данных.

4.3 СУиК осуществляет информационное обеспечение учета и контроля ЯМ, поступающих на предприятие, обращающихся на предприятии, убывающих с предприятия и уничтожаемых на основе правовой ответственности предприятия.

4.4 СУиК учитывает любое перемещение ЯМ между ЗБМ предприятия, любое изменение вида и формы материала, при котором меняется индекс (наименование) материала, детали, изделия с ЯМ.

4.5 СУиК предоставляет своевременную и достоверную информацию для осуществления учета, контроля, управления и планирования всей деятельностью по учету и контролю ЯМ на предприятии.

4.6 СУиК обеспечивает в каждой ЗБМ и по предприятию в целом:

- информационную запись всех измерений в ключевых точках измерений по количеству и иным характеристикам ЯМ;

- своевременное информационное сопровождение всех перемещений и превращений ЯМ в ЗБМ;

- информационное оповещение о ЯМ, поступающих в зону и покидающих ЗБМ;

- определение количества ЯМ в каждой зоне баланса и на предприятии в целом;

- составление, регистрацию и ведение учетных и отчетных данных и документов;

- информационное взаимодействие с административным руководством предприятия;

- контроль корректности операций по перемещению и изменению учетного вида ЯМ;

- контроль своевременности предоставления и поступления коррекций по контролю и учету ЯМ;

- учет персонала, имеющего доступ к ЯМ, и персонала, непосредственно осуществляющего учет и контроль ЯМ;

- контроль и учет доступа персонала к автоматизированным средствам, журналам по учету и контролю и к ЯМ;

- оперативный поиск местонахождения нужной продукции;

- информационную связь с системой физической защиты предприятия;

- защиту, в пределах своей компетенции, циркулирующей в СУиК информации;

- информационное взаимодействие в рамках учета и контроля ЯМ с системами учета и контроля других предприятий, информационными системами федеральных органов управления, государственной информационной системой учета и контроля ЯМ;

- необходимую информационную поддержку работ инвентаризационных и инспекционных комиссий;

- получение исходных данных для аналитической работы оценки качества учета, контроля и сохранности ЯМ на предприятии.

5 Общие требования к СУиК и режиму ее функционирования

5.1 СУиК должна выполнять следующие функции:

- административные:

1) обслуживание информационных запросов потребителей и администрации о состоянии работ на предприятии по обращению с ЯМ, о их наличии, местоположении и т.п.;

2) обеспечение контроля и управления разрешительной системой допуска к данным СУиК и к ЯМ;

3) информационную поддержку расследований по нештатным ситуациям, связанным с ЯМ;

- управление операциями и базами данных:

1) получение и обработка исходной информации о наличии и перемещениях ЯМ между зонами баланса, ядерными установками предприятия, между данным предприятием и предприятиями Минатома России, предприятиями других ведомств;

2) формирование баз данных по предприятию;

3) формирование выходной и отчетной информации в необходимых форматах и на нужных носителях;

4) контроль за взаимосогласованностью поступившей информации и сигнализация о найденных несоответствиях;

5) управление базами данных, оперативный поиск и выдача информации;

6) ведение работы по поддержке архивов и резервных копий баз данных.

5.2 Информационное обеспечение СУиК должно удовлетворять следующим требованиям:

- объективности - все учетные записи должны иметь документальное подтверждение;

- согласованности - вся документация по учету и контролю ЯМ и содержимое баз данных СУиК должны составлять единую систему; обмен информацией данного предприятия с внешними организациями должен вестись в согласованных формах и форматах;

- надежности хранения баз данных, включая сбои и отказы оборудования;

- своевременности - безотлагательная регистрация изменений учетных единиц, инвентарных количеств материалов. Отчетность по ним должна соответствовать требованиям отраслевой системы учета и контроля ЯМ;

- полноте - все перемещения, ведущие к изменению зарегистрированного количества ЯМ, должны регистрироваться системой;

- последовательности - информация о количестве ЯМ, зарегистрированного на определенную дату, в дальнейшем не может быть изменена. Исправление ошибочно введенных данных о ЯМ в базах данных должно производиться и фиксироваться по специально разработанной процедуре, исключающей возможность фальсификации;

- преемственности - автоматизированная система учета и контроля должна быть согласованной с существующей на предприятии системой учета и контроля на бумажных носителях.

5.3 Информационная подсистема должна содержать:

- полную информацию по количеству, составу, номенклатуре, месту нахождения ЯМ;

- документацию по учету и контролю ЯМ для каждого типа документа в течение времени, установленного в утвержденном порядке;

- сведения о планируемых мероприятиях по учету и контролю ЯМ на предприятии;

- информацию по составу и правам доступа персонала, осуществляющего непосредственный учет и контроль ЯМ; сведения о технических характеристиках ядерной установки в пределах, необходимых для учета и контроля ЯМ;

- сведения о технических характеристиках контролирующей измерительной аппаратуры.

5.4 Информационная подсистема должна обеспечивать выполнение следующих функций:

- хранение информации о ЯМ;

- обработку данных по ЯМ;

- подготовку отчетных данных;

- формирование отчетов;

- контроль на отсутствие ошибок и достоверность;

- подготовку отчетов для передачи в информационный центр;

- выдачу учетных и отчетных форм исполнителям;

- контроль своевременности предоставления отчетов и выдачи отчетных документов;

- контроль корректности операций с ЯМ в каждой зоне баланса материалов;

- контроль своевременности ввода данных;

- выдачу статистической информации по базе данных о ЯМ.

5.5 Информационная подсистема должна быть системой нормального функционирования, т.е. аварийный выход ее из строя или отключение не должны наносить ущерба учету ЯМ на предприятии.

5.6 Степень автоматизации учета и контроля ЯМ определяют на каждом предприятии конкретно.

6 Требования к информационному обеспечению

6.1 Информационное обеспечение должно включать:

- входную информацию;

- информацию по внутренним перемещениям;

- выходную информацию;

- нормативно-справочную информацию.

6.2 Входная информация должна включать:

- перечень зон баланса ЯМ с информацией о процедурах учета, контроля и системах контроля доступа;

- учетные и отчетные документы по каждой зоне баланса ЯМ и по предприятию в целом за прошедший период времени, определенный установленным порядком;

- документы, содержащие данные инспекций и проверок;

- специальная информация, относящаяся к обеспечению учета и контроля ЯМ.

Система должна обеспечивать ввод:

- паспортных данных ЯМ, поступающих на предприятие с сопроводительной документацией;

- паспортных данных создаваемых на предприятии новых учетных единиц;

- результатов измерений;

- изменения характеристик ЯМ, произошедших в процессе технологической обработки;

- данных о перемещениях учетных единиц;

- информации о смене материально-ответственных лиц;

- данных об изменении прав доступа персонала СУиК;

- различной справочной информации (списки поставщиков и потребителей, возможные типы контейнеров, списки персонала, структура мест хранения и т.п.);

- информации о распорядительных документах по предприятию, ядерной установке (о проведении инвентаризации, о приеме очередной партии контейнеров и т.д.);

- результатов сверок и инвентаризаций, а также результатов разборки нештатных ситуаций.

6.3 Выходная информация должна включать:

- данные по количеству, составу, номенклатуре, месту нахождения ЯМ;

- отчет о фактически наличном количестве ЯМ;

- отчет об изменении инвентарного количества ЯМ;

- материально-балансовый отчет;

- другие виды отчетов (инспекционный, в МАГАТЭ, специальный отчет, в случае необходимости, и т.д.).

Система должна обеспечить:

- вывод принятых на предприятии форм учетных и отчетных документов (с возможностью просмотра на экране дисплея и/или печати на принтере);

- перевод принятых на установке форм учетной и отчетной документации в другие формы отчетности и выборку данных по запросу в удобной форме;

- подготовку паспорта отправляемого с предприятия контейнера, сформированного в виде файла (в формате, согласованном с принимающим предприятием);

- обслуживание информационных запросов операторов и администрации предприятия, инвентаризационных и инспекционных комиссий о наличии ЯМ, о состоянии работ с ЯМ, на выдачу различных сводок, статистических отчетов, на выдачу подробной или выборочной информации о заданной учетной единице. Обслуживание информационных запросов следует производить с учетом прав доступа пользователя к данным;

- выдачу (на принтер или на магнитный носитель) статистических отчетов, сводок и документов, а также иных необходимых данных для обеспечения отчетности предприятия;

- передачу (при включении СУиК предприятия в информационную систему более высокого уровня) в вычислительную сеть более высокого уровня балансовых и других обобщающих данных.

6.4 Хранение и восстановление данных должны отвечать следующим требованиям:

- данные необходимо хранить в одной или нескольких базах данных СУиК, резервные копии которых поддерживают и регулярно обновляют;

- данные должны быть сгруппированы в таблицы по назначению, степени секретности, частоте использования или другим признакам с тем, чтобы по возможности уменьшить сетевой трафик;

- информацию об ушедших с предприятия ЯМ, историю каждой учетной единицы для обеспечения возможности восстановления последовательности проведенных с ЯМ действий необходимо постоянно хранить в соответствующих базах данных;

- необходимо постоянно хранить контрольные журналы работы всех операторов СУиК. Данные контрольных журналов могут быть скорректированы с сохранением каждой измененной записи по принятой методике.

6.5 Учет ЯМ, предназначенных для использования в оборонных целях, и учет ЯМ, предназначенных для использования в мирных целях, ведут раздельно, с выдачей отчетной информации в соответствующую центральную информационную систему Минатома России.

6.6 Сбор информации из зон баланса ЯМ в центральную базу данных СУиК информационной подсистемы предприятия осуществляется по имеющимся каналам связи (по локальной компьютерной сети системы учета ЯМ предприятия, с помощью бумажных или магнитных носителей и др.), а сбор конфиденциальной информации - по защищенным каналам связи, либо иным способом, исключающим возможность получения ее посторонними лицами.

6.7 Передача конфиденциальной информации в Федеральную информационную систему учета ЯМ Минатома России, по запросам в установленном порядке других федеральных и региональных органов управления, федеральных и региональных органов надзора, между предприятиями Минатома России, воинскими частями Министерства обороны и предприятиями других ведомств осуществляется по защищенным каналам связи.

6.8 Формы отчетной документации, вид и типы форм для документов внешних инспекционных комиссий устанавливаются отраслевыми документами.

6.9 Выдача отчетной информации в Федеральную информационную систему учета ЯМ Минатома России должна осуществляться согласно установленному регламенту, либо оперативно в соответствии с утвержденной сводкой оперативных донесений. Процедура передачи информации должна осуществляться во взаимно согласованных с центральной системой режимах.

7 Требования к базовому программному обеспечению

7.1 Базовое программное обеспечение СУиК должно быть сертифицировано для применения в автоматизированных системах требуемого класса защищенности от несанкционированного доступа.

7.2 Операционная система должна содержать и обеспечивать:

- средства работы в сети;

- средства межзадачной связи, в том числе сетевые;

- средства защиты данных от несанкционированного доступа:

1) контроль доступа при входе в систему;

2) защиту памяти;

3) разделение и учет доступа к ресурсам;

- средства обработки ошибок;

- средства поддержки работоспособности системы;

- развитые средства доступа к базам данных;

- поддержку наиболее распространенных сетевых протоколов;

- устойчивость к сбоям аппаратуры;

- возможности сбора статистических данных о работе системы.

7.3 Операционная система может также содержать:

- поддержку технологии "клиент-сервер";

- мультизадачность с наличием системы приоритетов и квантованием по времени;

- возможность сетевой дистанционной загрузки рабочих станций;

- поддержку использования источника бесперебойного питания.

7.4 Система управления базами данных должна содержать удобные средства создания резервных копий и их использования для восстановления, а также, при необходимости, может содержать:

- удобный интерфейс пользователя;

- средства автоматической репликации баз данных.

7.5 Система управления базами данных должна обеспечивать:

- поддержку работы в сети;

- высокое быстродействие и производительность;

а также, при необходимости, может обеспечивать:

- наличие ODBC-драйвера (Open DataBase Connectivity - связь открытых баз данных) для интерфейса с другими базами данных, совместимых с ODBC;

- обеспечение защищенности данных и разграничения доступа к ним;

- поддержку структурированного языка запросов SQL, являющегося стандартом IBM для работы с базами данных.

7.6 Инструментальные средства программирования должны предоставлять разработчику:

- удобные средства разработки программ;

- возможности визуального программирования;

- хорошие средства отладки;

- развитый аппарат обработки ошибок;

- поддержку многооконности;

- удобные средства связи с базами данных.

8 Требования к прикладному программному обеспечению

8.1 Прикладное программное обеспечение должно выполнять следующие функции:

- обеспечение учета и контроля ЯМ, состав которых определяется для данного предприятия соответствующими документами и инструкциями;

- сбор и обработка информации об изменении характеристик, результатах измерений и движении ЯМ, как правило, в диалоговом режиме, близком к реальному времени;

- обеспечение возможности для включения в системы более высокого уровня (открытость);

- обеспечение возможностей совершенствования программного комплекса без нарушения общей логики (модульность);

- обеспечение настраиваемости на возможные изменения в зонах баланса ЯМ;

- обеспечение возможности модификаций с целью:

1) расширения состава функций;

2) подключения новых типов устройств;

3) включения в обслуживание СУиК дополнительных технологических участков;

4) включения в системы более высоких уровней;

5) перехода на совместимые более современные компьютеры;

- удобный стандартизованный интерфейс пользователя, обеспечивающий работу в диалоговом режиме с использованием систем меню;

- обеспечение возможности использования унифицированных протоколов измерений приборами неразрушающего контроля.

8.2 Состав и назначение модификаций должны базироваться на результатах анализа функционирования СУиК и быть направлены на повышение эффективности выполняемых системой задач. Такие модификации не должны требовать значительного перепрограммирования. Дополнение и модернизация СУиК должны происходить без нарушения ее функционирования и ухудшения ее эксплуатационных характеристик.

9 Требования к техническому обеспечению

9.1 Требования к аппаратным средствам

Аппаратные средства системы СУиК должны состоять из двух групп:

- компьютерное оборудование;

- сетевое оборудование.

9.2 Требования к компьютерному оборудованию

9.2.1 Компьютерное оборудование выбирают, исходя из:

- соответствия решаемым СУиК задачам и выбранной базовой программной платформы;

- соотношения стоимости к производительности;

- степени распространения в России;

- наличия долгосрочной перспективы серийного промышленного производства;

- перспектив в усовершенствовании и автоматизации СУиК ЯМ.

9.2.2 По функциональному назначению в системе СУиК компьютеры делят на серверы, рабочие станции технологических участков, пульты управления, административно-информационные консоли и др. Рабочие станции должны иметь возможность подключения достаточного количества внешних каналов ввода-вывода. Конкретные спецификации компьютеров определяют исходя из их назначения в системе, объема хранимой и циркулирующей в системе информации, состава подключаемых внешних устройств.

9.3 Требования безопасности для компьютерного оборудования

9.3.1 Компьютерное оборудование следует устанавливать в закрытых отапливаемых помещениях. В окружающей среде не должно быть паров агрессивных веществ, вызывающих коррозию, температура окружающего воздуха должна быть от 10 до 35 °С, относительная влажность окружающего воздуха при температуре 30 °С - от 40% до 80%, атмосферное давление - от 630 до 800 мм рт.ст. Питание должно осуществляться от однофазной сети переменного тока напряжением (220±22) В, частотой (50,0±0,5) Гц. Напряженность внешнего электромагнитного поля должна быть не более 3 В/м в диапазоне частот от 0,15 до 300,00 МГц.

9.3.2 Электропитание компьютеров осуществляют через источник бесперебойного питания с использованием отдельной трехпроводной электролинии, к которой не должно быть подключено сильноточное и коммутационное электрооборудование.

В сети не должно быть импульсных помех, провалов и прерывания питания.

9.3.3 Заземление должно быть выполнено с учетом требований нормативных документов, действующих на предприятии.

9.4 Требования к сетевому оборудованию

9.4.1 Сетевое оборудование должно соответствовать промышленным стандартам.

9.4.2 Сигнальные линии локальной сети должны быть проложены (с резервированием) двумя кабелями, по своим электрическим параметрам соответствующими "категории 5" (Level 5) классификации фирмы AT&T.

9.4.3 Трассы линий связи должны пролегать в отдельных кабельгонах на расстояниях, исключающих взаимодействие с силовыми линиями электропитания.

9.4.4 Связи между системами, содержащими данные разного уровня конфиденциальности, должны осуществляться через сетевые маршрутизаторы, которые должны обеспечивать все необходимые меры административного контроля и гарантировать разделение информационных потоков и защиту от несанкционированного доступа из одной системы в другую.

9.4.5 Взаимодействие между удаленными станциями должно быть осуществлено посредством оптоволоконных линий связи или с применением обычных проводных соединений, но используя модемы. Первый способ является более предпочтительным из-за гораздо более высокой скорости обмена данными, большой помехозащищенности и обеспечения защиты передаваемой информации от несанкционированного доступа.

9.4.6 В составе приборного оснащения СУиК обязательно должны быть диагностические устройства для проверки качества линий связи, определения уровня помех и отыскания обрывов и коротких замыканий в них (сетевые сканеры или анализаторы).

9.4.7 Электропитание сетевых устройств должно осуществляться от источников бесперебойного питания.

9.5 Требования к регистрирующему оборудованию, не входящему в состав аппаратного оснащения СУиК

9.5.1 Для регистрирующего оборудования, не входящего в состав аппаратного оснащения СУиК (взвешивающие устройства, устройства для считывания бар-кодов и т.д.), должны нормироваться технические параметры:

- диапазон регистрации;

- погрешность регистрируемой величины;

- среднее время наработки на отказ;

- периодичность и сроки контрольных проверок аппаратуры;

- конкретные технические параметры (ударная прочность и т.п.);

- интерфейс связи с ЭВТ.

10 Требования к системе защиты информации

10.1 Обращение с информацией в СУиК должно удовлетворять требованиям нормативных документов, регламентирующих порядок защиты государственной тайны.

10.2 Система защиты информации должна быть составной частью СУиК, так как циркулирующая в СУиК информация является чувствительной по отношению к несанкционированным действиям. На всех этапах функционирования СУиК (передача, сбор, обработка, анализ, хранение данных) защита информации должна быть обеспечена применением комплекса мероприятий по предотвращению утечки информации или исключению воздействия на нее по техническим каналам, по предупреждению преднамеренных программно-технических воздействий с целью нарушения целостности (уничтожения, искажения) информации в процессе ее обработки, передачи и хранения или нарушения работоспособности технических средств.

10.3 Основными направлениями обеспечения информационной безопасности должны быть:

- обеспечение защиты информации от хищения, утраты, утечки, уничтожения, искажения и подделки посредством несанкционированного доступа и специальных программно-технических воздействий;

- обеспечение защиты информации от утечки за счет побочных электромагнитных излучений и наводок от средств обработки защищаемой информации на различные коммуникации.

10.4 Система защиты информации должна предусматривать комплекс организационных, программных, технических и криптографических средств и мер по защите информации в СУиК как в процессе документооборота на бумажных носителях, так и при автоматизированной обработке, хранении и передаче по каналам связи, при ведении разговоров, раскрывающих информацию с ограниченным доступом, при использовании импортных технических и программных средств.

10.5 В отрасли основные требования по защите информации, порядок разработки, введения в действие и эксплуатации автоматизированных систем в защищенном исполнении определены инструкцией [2].

10.6 В целях дифференцированного подхода к защите информации в СУиК проводят:

- классификацию автоматизированных систем, предназначенных для обработки защищаемой информации;

- категорирование технических средств и систем, предназначенных для обработки, передачи и хранения секретной информации.

10.7 На предприятиях требования по защите информации в СУиК от несанкционированного доступа должны быть определены на основании руководящего документа [3], исходя из конкретных условий функционирования:

- наличия в системе информации различного уровня конфиденциальности и чувствительности по отношению к несанкционированным действиям;

- уровня полномочий персонала СУиК на доступ к конфиденциальной информации;

- режима обработки данных в СУиК (коллективного или индивидуального).

Эти признаки определяют класс защищенности СУиК.

10.8 Категорию технических средств и систем определяют в установленном порядке в зависимости от степени секретности обрабатываемой (передаваемой, хранимой) информации и условий ее расположения.

10.9 Уровень полномочий пользователей и персонала СУиК определяют в соответствии с действующей на предприятии разрешительной системой допуска исполнителей к секретным документам и сведениям.

10.10 Конкретные средства и меры защиты информации определяют на предприятии по результатам предпроектного обследования объекта автоматизации, сертификационных испытаний средств защиты информации и специальных исследований технических средств и систем, исходя из установленного класса защищенности СУиК и категории технических средств и систем, предназначенных для обработки секретной информации.

10.11 При решении вопросов защиты информации в СУиК необходимо руководствоваться требованиями следующих документов:

- законов РФ [4], [5], [6], [7];

- ГОСТ 28147, ГОСТ Р 34.10, ГОСТ Р 34.11;

- руководящих документов [8], [9], [10];

- положений [11], [12], [13], [14], [15], [16];

- рекомендации [17];

- правил [18], [19].

10.12 Контроль состояния и эффективности защиты информации должны проводить с применением технических средств контроля.

11 Требования надежности

11.1 Полная потеря информации в СУиК в условиях нормальной эксплуатации и при проектных авариях должна быть исключена посредством организации и поддержки системы хранения и восстановления данных, к которой относят:

- дублирование сервера или использование дублирования на жестких магнитных дисках (RAID-технология);

- хранение на предприятии дистрибутивных копий как базового, так и прикладного программного обеспечения;

- хранение резервных копий баз данных. Необходимо иметь не менее двух наборов поочередно используемых внешних носителей для резервных копий, которые необходимо

хранить отдельно либо в хранилище файлов, либо (и), по соответствующему соглашению, в другом компьютерном центре.

11.2 Время восстановления работоспособного состояния СУиК - не более 10 ч, и должно быть уточнено для каждой конкретной подсистемы на стадии разработки технического задания на разработку СУиК.

11.3 Среднее время наработки на сбой определяют в нормативных документах на каждую конкретную систему, и оно должно быть не менее 250 ч.

11.4 Время наработки на отказ оборудования определяют гарантиями изготовителей и оно должно быть не менее указанного в требованиях надежности по ГОСТ 27201 с отнесением ЭВТ к пятому классу.

11.5 При проектировании размещения и эксплуатации оборудования информационной подсистемы должны выполняться требования пожарной и общепромышленной безопасности по ГОСТ 12.4.009, ГОСТ 12.1.004.

12 Требования к организационному обеспечению

12.1 Организационное обеспечение системы должно быть определено документами, устанавливающими организационную структуру, права и обязанности пользователей и персонала, эксплуатирующего СУиК.

Эти документы (инструкции, положения, приказы и т.д.) должны определять:

- функции, права и обязанности персонала по обеспечению функционирования СУиК, в том числе по профилактике оборудования;

- действия персонала при отказах и сбоях технических и программных средств;

- действия персонала в специфических случаях;

- действия персонала по восстановлению работоспособности системы;

- ответственность должностных лиц, персонала и пользователей.

12.2 Для обслуживания СУиК необходимы прикладные и системные программисты и инженеры-электроники. Уровень подготовки, квалификация и количество специалистов определяет предприятие с учетом возможностей обеспечения финансовыми, материальными и людскими ресурсами.

12.3 На предприятиях должны быть разработаны программы обучения и повышения квалификации специалистов, обеспечивающих функционирование СУиК ЯМ.

13 Требования к порядку разработки, вводу в действие и эксплуатации

13.1 При разработке СУиК ЯМ следует руководствоваться нормативными документами в соответствии с разделом 2 и документами [1]-[19].

13.2 На предпроектной стадии проводят обследование объекта автоматизации, завершающееся разработкой технико-экономического и аналитического (с точки зрения защиты информации) обоснования разработки СУиК. Выпускают техническое задание на разработку СУиК, включающее конкретные требования по защите информации.

Указанные документы согласовывают и утверждают в установленном в отрасли порядке.

13.3 Стадия проектирования СУиК завершается разработкой проекта, включающего организационные и технические решения, разработку программной среды СУиК, средств и мер защиты информации, отвечающих требованиям настоящего стандарта и требованиям технического задания на разработку СУиК.

13.4 Технические средства должны пройти:

- испытания смонтированных технических средств на работоспособность в местах установки;

- проверку на соответствие требованиям по защите информации.

13.5 Базовое и прикладное программное обеспечение должно пройти комплекс лабораторных испытаний.

13.6 Применяемые средства защиты информации должны иметь сертификат соответствия требованиям по защите информации.

13.7 Перед стадией эксплуатации СУиК необходимо:

- разработать ведомость эксплуатационных документов;

- представить общее описание системы, включающее ее основные характеристики и сведения об эксплуатации, областях применения, требуемых технических средствах;

- разработать комплекс рабочей документации (положения, инструкции, графики, схемы, перечни и т.д.);

- представить описание комплекса организационно-технических мероприятий, организационной структуры и штатного расписания предприятия в части, касающейся СУиК;

- разработать руководство системного программиста по ГОСТ 19.001, ГОСТ 19.101, ГОСТ 19.103, включающее сведения для установки, настройки, тестирования системы, а также восстановления после аварий;

- разработать руководства пользователей по ГОСТ 19.001, ГОСТ 19.101, ГОСТ 19.103, содержащие сведения для обеспечения диалога пользователей с программно-аппаратным оснащением СУиК;

- представить акт приемки в эксплуатацию программного обеспечения;

- представить план-график ввода СУиК в эксплуатацию.

13.8 На этапе ввода в действие в установленном порядке проводят аттестацию программно-аппаратного оснащения СУиК на соответствие требованиям по защите информации.

13.9 Перед стадией опытной эксплуатации системы выпускают акт комиссии о приемке программно-аппаратного оснащения СУиК в опытную эксплуатацию.

13.10 Приемку программно-аппаратного оснащения СУиК в промышленную эксплуатацию проводит комиссия, включающая представителей разработчика, заказчика, эксплуатирующей организации. Если программно-аппаратное оснащение СУиК имеет выход в центральную информационную систему, то в состав комиссии вводят представителя инспектирующей организации. По результатам приемки должен быть составлен акт технической приемки.

Приложение А
(справочное)

Библиография

[1] Концепция системы государственного учета и контроля ядерных материалов. Одобрена постановлением Правительства РФ 14 октября 1996 г. N 1205.

[2] Временная типовая инструкция по защите информации в автоматизированных системах предприятий и организаций Минатома России. Утверждена приказом Министра от 14.12.99 N 769.

[3] Руководящий документ Гостехкомиссии России. Автоматизированные системы. Защита от несанкционированного доступа к информации. Классификация автоматизированных систем и требования по защите информации. Утвержден председателем Гостехкомиссии России 30.03.92 учетный N 2/9-71Д.

[4] Закон РФ "Об информации, информатизации и защите информации" от 20.02.95 N 24-ФЗ.

[5] Закон РФ "О государственной тайне" от 21.07.93 N 5485-1.

[6] Закон РФ "О сертификации продукции и услуг" от 10.06.93 N 5151-1.

[7] Закон РФ "О стандартизации" от 10.06.93 N 5154-1.

[8] Руководящий документ. Средства вычислительной техники. Межсетевые экраны. Защита от несанкционированного доступа к информации. Показатели защищенности от несанкционированного доступа к информации. Утвержден Председателем Государственной технической комиссии при Президенте РФ 25.07.97.

[9] Руководящий документ Гостехкомиссии России. Требования по защите от несанкционированного доступа к информации в автоматизированных системах учета и контроля ядерных материалов. Утверждены заместителем Министра РФ по атомной энергии от 30.01.97 N 2/9-8.

[10] Руководящий документ. Общие требования по защите информации в системах физической защиты ядерно-опасных объектов. Утвержден приказом Минатома от 06.04.99 N 227.

[11] Положение о государственном лицензировании деятельности в области защиты информации. Утверждено решением Гостехкомиссии при Президенте РФ и Федерального агентства правительственной связи и информации при Президенте РФ от 27.04.94 N 10 и введено приказом Министра от 08.07.94 N 296.

[12] Положение о сертификации средств защиты информации. Утверждено постановлением Правительства РФ от 26.06.95 N 608 и введено приказом Министра от 30.10.95 N 447.

[13] Положение по аттестации объектов информатики предприятий и организаций Минатома России на соответствие требованиям безопасности информации. Утверждено приказом Министра от 07.02.94 N 51.

[14] Типовое положение об органе по аттестации объектов информатики Минатома России на соответствие требованиям безопасности информации. Утверждено приказом Министра от 06.04.94 N 142.

[15] Положение об аккредитации органов по аттестации объектов информатики Минатома России на соответствие требованиям безопасности информации. Утверждено приказом Министра от 06.04.94 N 142.

[16] Положение об учете и контроле ядерных материалов в Министерстве РФ по атомной энергии. Утверждено приказом Минатома от 15.05.2002 N 227.

[17] Методические рекомендации. Аттестационные испытания автоматизированных систем по требованиям безопасности информации. Утверждены приказом Министра от 06.04.94 N 142.

[18] Правила физической защиты ядерных материалов, ядерных установок и пунктов хранения ядерных материалов. Утверждены постановлением Правительства РФ от 07.03.97 N 264.

[19] Правила по проведению сертификации в РФ. Утверждены постановлением Госстандарта России от 16.02.94 N 3.