ФЕДЕРАЛЬНОЕ АГЕНТСТВО ПО ОБРАЗОВАНИЮ

МОСКОВСКИЙ ИНЖЕНЕРНО-ФИЗИЧЕСКИЙ ИНСТИТУТ
(ГОСУДАРСТВЕННЫЙ УНИВЕРСИТЕТ)

В.В. Кондаков А.А. Краснобородько

ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ СИСТЕМ ФИЗИЧЕСКОЙ ЗАЩИТЫ, УЧЕТА И КОНТРОЛЯ ЯДЕРНЫХ МАТЕРИАЛОВ

Рекомендовано УМО «Ядерные физика и технологии»
в качестве учебного пособия
для студентов высших учебных заведений

Москва 2008

УДК 004.77:621.039.5(075)
ББК 31.46я7
К64

Кондаков В.В., Краснобородько А.А. **Информационная безопасность систем физической защиты, учета и контроля ядерных материалов:** *Учебное пособие*. М.: МИФИ, 2008. 48 с.

В пособии рассмотрены основные вопросы, связанные с обеспечением информационной безопасности систем физической защиты, учета и контроля ядерных материалов. Рассматриваются основные угрозы информационной безопасности и способы противодействия им. Приводится содержание основных нормативных документов в области обеспечения информационной безопасности автоматизированных систем.

Данное учебное пособие предназначено для студентов, специализирующихся в области физической защиты, учета и контроля ядерных материалов. Пособие подготовлено для методического обеспечения магистерской образовательной программы «ФЗУиК ЯМ» направления «Техническая физика» и для подготовки инженеров-физиков по специальности 651000 направления «Ядерные физика и технологии» и по специальности 140309 «Безопасность и нераспространение ядерных материалов».

Пособие подготовлено в рамках Инновационной образовательной программы.

Рецензент канд. техн. наук И.Г. Меринов

ISBN 978-5-7262-1071-1

Редактор Н.Н. Антонова
Компьютерная верстка Г.А. Бобровой

Подписано в печать 20.11.2008 Формат 60x84 1/16
Печ.л. 3,0 Уч.-изд.л. 3,0 Тираж 150 экз. Изд. № 4/52
Заказ № 2-2414

Московский инженерно-физический институт (государственный университет).
115409 Москва, Каширское шоссе, 31

Типография издательства «Тровант»
г. Троицк Московской области

СОДЕРЖАНИЕ

ВВЕДЕНИЕ

Данное учебное пособие предназначено для студентов, специализирующихся в области учета и контроля и физической защиты ядерных материалов и посвящено вопросам создания и эксплуатации компьютеризированных систем учета и контроля ядерных материалов (КСУиК ЯМ) и их физической защиты (ФЗ ЯМ). Предмет рассмотрения очень обширен. В него входят изучение нормативных документов, включая стандарты информационной безопасности, основные понятия в сфере организации и оборудовании локальных компьютерных сетей, операционные системы компьютеров, теория и практика управления базами данных, программирование на языках высокого уровня. Специалисты, призванные проектировать и поддерживать системы такого рода, должны обладать знаниями в области теории проектирования компьютеризированных систем, представлять себе процедуры сбора информации, оценки данных и принятия решений. Они должны знать существующие отраслевые стандарты и мировую практику создания сложных информационных систем. В рамках выделенного для изучения курса времени подробное рассмотрение всех этих вопросов невозможно.

Поэтому в качестве цели при составлении данного курса было выбрано получение слушателями представления о методах и технологиях создания современных компьютеризированных систем учета и контроля ядерных материалов (КСУиК ЯМ); автоматизированных системах сбора и обработки информации в комплексах физической защиты; знакомство с необходимым для их создания и эксплуатации программным обеспечением (ПО) и обзор современных систем учета и контроля, основанных на различных принципах. Курс базируется на знаниях, полученных слушателями в курсе «Учет и контроль ядерных материалов». Он не предназначен для подготовки специалистов в области информационных технологий и программирования.

Основная цель мероприятий по учету ядерного материала (ЯМ) – своевременное обнаружение недостач или излишков ЯМ, случаев потерь, хищений и несанкционированного использования ЯМ, а также выявления причин и источников появления таковых. Учет –

одно из мероприятий, обеспечивающих выполнение этой цели, наряду с контролем и физической защитой. Другой обязанностью систем учета есть предоставление органам государственной власти и другим официальным уполномоченным органам информации, необходимой для выполнения ими своих обязанностей.

Полноценное достижение этих целей невозможно без автоматизации процессов сбора и обработки информации.

Требования, предъявляемые Федеральной информационной системой (ФИС) к отчетности предприятий ядерной отрасли, как по объему информации, так и по времени ее предоставления, не могут быть удовлетворены без использования современных информационных технологий.

КСУиК ЯМ, создаваемые на предприятиях, имеющих в обращении ядерные материалы, вместе с центральной компьютеризированной системой сбора и обработки информации образуют Федеральную информационную систему. Все требования, которые предъявляет ФИС к отчетности, детализации информации и периодичности ее представления, накладывает жесткие ограничения на функциональность и программное обеспечение КСУиК ЯМ на предприятиях.

1. ПРОБЛЕМЫ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ В КОМПЬЮТЕРИЗИРОВАННЫХ СИСТЕМАХ

Проблема безопасности информационных технологий в последние годы постоянно обостряется. Аналитические обзоры демонстрируют каждый год рост ущерба от нарушения безопасности. Стремительное развитие информационных технологий приводит к отставанию теории и практики обеспечения безопасности от прогресса в сфере технологий. Огромная вычислительная мощь современных вычислительных систем сочетается с простотой их эксплуатации. Создание глобальной информационной среды обеспечивает доступ к информационным ресурсам огромного количества пользователей различной квалификации. Большинство пользователей не обладают достаточной квалификацией для поддержания безопасности компьютерных систем на должном уровне. Многие эпидемии компьютерных вирусов смогли реализоваться по той причине, что пользователи не производят регулярной проверки своих компьютеров, не обновляют антивирусные базы данных и своевременно не устанавливают обновления операционных систем, которые ликвидируют выявленные ошибки в программном обеспечении. При этом процессы производства, распространения, внедрения информации и оценки результатов информационного воздействия стали носить промышленный характер, они поставлены на конвейер. Информатизация на базе внедрения компьютерных и телекоммуникационных технологий является реакцией общества на потребность в существенном увеличении производительности труда. Таким образом, создание компьютерных систем сбора, обработки и передачи информации является объективной тенденцией, в том числе и в таких «чувствительных» областях, как ядерная безопасность и контроль за ядерными материалами.

Широкое внедрение персональных компьютеров и их использование в ядерной отрасли приводит к необходимости учета возникающих при этом новых видов угроз. Средства автоматизированной обработки информации с использованием персональных компьютеров и сетей связи имеют ряд особенностей, позволяющих бесконтрольно манипулировать информацией соответствующих автоматизированных систем (АС) как персоналу, так и посторонним лицам, а также скрытно получать доступ к обрабатываемой

информации. Поэтому конфиденциальная информация без адекватной ее защиты может быть достаточно легко скомпрометирована, вызвав значительные потери для владельца такой информации. В связи с этим ввод и обработка информации ограниченного доступа в любых автоматизированных системах должна происходить с учетом определенного риска и сопровождаться привлечением соответствующих средств и мер защиты.

Применительно к АС, наиболее опасными событиями по отношению к обрабатываемой информации являются: утрата, раскрытие (разглашение), порча, кража, подделка (искажение), блокирование информации. Также угрозой является нарушение работы системы обработки информации. Все эти события могут быть результатом преднамеренных или непреднамеренных действий как законных, так и незаконных пользователей АС. Часть угроз безопасности компьютеризированные системы наследуют от традиционных систем обработки информации, например, кражу или разглашение информации. Но вместе с тем в результате компьютеризации появляются новые угрозы. Это определяется тем, что автоматизация обработки информации связана с отстранением человека от непосредственной работы с носителем информации. Полномочия передаются компьютерным программам, которые в результате умышленных действий или вследствие ошибок в программном коде могут нарушать регламент обработки конфиденциальной информации. Чтобы компьютерная система могла использоваться для автоматизации обработки конфиденциальной информации, она должна успешно противостоять угрозам безопасности.

На ядерных объектах, согласно нормативным отраслевым документам, должен быть ограничен доступ к информации, содержащейся в автоматизированной системе учета и контроля ядерных материалов (АСУиК ЯМ) и сведениям о составе и функционировании системы физической защиты (СФЗ) объекта, частью которой является компьютеризированная система [1–4]. Обработка секретной информации осуществляется на основании нормативных документов, которые регламентируют порядок защиты информации, составляющей государственную тайну. Однако при переходе от обработки бумажных документов к компьютерной обработке информации необходимо обеспечить преемственность выполнения этих требований. Компьютеризированная система, предназначен-

ная для обработки секретной информации должна удовлетворять требованиям этих документов. Например, необходимо организовывать систему доступа пользователей к информации в компьютеризированных системах в соответствии с грифом секретности документа и уровня доступа сотрудника использовании.

Уязвимость информации, обрабатываемой и/или хранящейся в компьютерной памяти, резко увеличивается с ростом количества персональных компьютеров, объединяемых в различного рода сети. Данные в отдельном компьютере доступны только при наличии физического доступа к нему (конечно, существуют возможности съема информации с автономного работающего устройства по его электромагнитному излучению, наводкам или оптическому каналу, но эти угрозы подробно не рассматриваются в данном пособии). Подключение персональных компьютеров, которыми в массовом порядке оснащаются рабочие места персонала предприятий и объектов, имеющих дело с ядерными материалами, даже к локальным сетям приводит к существенному расширению инструментария для потенциальных нарушителей целостности информации. Большинство нарушений, как показывает отечественный и зарубежный опыт, связано именно с проникновением в компьютерные сети, что практически сводит на нет эффективность стандартных процедур физического ограничения доступа к компьютеру.

В настоящее время в РФ имеется достаточно проработанная система стандартов в области обеспечения безопасности информации. Система, использующаяся для обработки информации ограниченного доступа (для СФЗ и УиК ЯМ эта информация часто является секретной), должна удовлетворять требованиям критериев этих стандартов. Это соответствие должно быть подтверждено аттестационными испытаниями. Кроме государственных стандартов действуют отраслевые стандарты и руководящие документы на уровне предприятия. Требования этих документов также необходимо принимать во внимание.

Таким образом, защищенная система обработки информации [5], в частности компьютеризированная СУиК ЯМ или система управления ФЗ, должна удовлетворять следующим трем требованиям:

• осуществлять автоматизацию процесса обработки конфиденциальной информации, включая все аспекты этого процесса связанные с обеспечением безопасности обрабатываемой информации;

• успешно противостоять угрозам безопасности, действующим в определенной среде;

• соответствовать требованиям и критериям стандартов информационной безопасности.

Немаловажно, чтобы системы защиты данных обеспечивали безопасность информации без существенного усложнения работы пользователя.

Таким образом, защищенные системы обработки информации должны обеспечивать информационную безопасность. Под информационной безопасностью специалисты понимают состояние защищенности информационной среды, обеспечивающее ее формирование и развитие в интересах организации и государства. Для предотвращения угроз информационной безопасности и устранению их последствий осуществляется комплекс организационных, правовых, технических и технологических мер, которые в совокупности называются мерами по защите информации. Основная их задача – предотвращать нежелательный доступ к аппаратуре, данным и программному обеспечению.

2. УГРОЗЫ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ И ПРОТИВОДЕЙСТВИЕ ИМ

Угрозами информационной безопасности называются факторы, стремящиеся нарушить нормальное функционирование системы. Угрозы могут быть как целенаправленные (субъективные), так и случайные (объективные). Российские стандарты в основном обращают внимание на целенаправленные угрозы, то есть на защиту информации от несанкционированного доступа (НСД). Не меньшую угрозу нормальному функционированию информационных систем могут представлять объективные факторы. Так, нарушение целостности данных в результате некачественного проектирования базы данных может свести ценность накопленных данных к нулю. Аналогичным образом возможна полная потеря информации в результате аппаратной аварии, если не предпринимались специальные меры по ее архивации и дублированию.

Можно выделить три широких класса вида угроз:

• угрозы конфиденциальности;

• угрозы целостности;

• угрозы отказа в обслуживании.

Противодействие объективным угрозам относится к вопросам обеспечения надежности системы. Противодействие субъективным угрозам является основной задачей обеспечения информационной безопасности

Специалисты в области защиты информации рассматривают различные способы воздействия угроз на компьютеризированную информационную систему. Выделяют информационные, программно-математические, физические и организационно-правовые способы воздействия.

Под информационными способами воздействия понимается всякого рода несанкционированное манипулирование информацией, содержащейся в базах данных. Сюда включается незаконный доступ к данным, хищение и копирование информации, сокрытие информации, ее намеренное искажение и нарушение технологии и своевременности ее обработки.

Программно-математические способы воздействия сводятся к воздействию на защищаемую систему с помощью внедряемых вредоносных программ или аппаратных устройств. Эти программы или устройства способны реализовывать недокументированные функции, что приводит к хищению или порче данных. В связи с тем, что в настоящее время при создании АС используется в основном импортное оборудование и программное обеспечение, произведенное зарубежными компаниями, вероятность внедрения специальных «закладок» достаточна велика. Более того, известны реальные случаи таких действий. Широко распространенное в настоящее время воздействие на компьютеры посредством компьютерных вирусов является одной из форм программно-математического воздействия угроз информационной безопасности.

Физические способы воздействия осуществляются через физическое воздействие различных факторов на вычислительную технику, сетевое оборудование, носители информации и, в конечном итоге, на персонал, осуществляющий работу с конфиденциальной информацией, и охранные системы. По оценкам Ассоциации защиты информации США 39% причин сбоев в работе компьютерных

систем являются физические угрозы. Физическое воздействие может быть организовано посредством высокотехнологической электронной аппаратуры, которая может перехватывать сигналы от работающего оборудования и таким образом похищать информацию. Возможно блокирование сигналов и нарушение нормальной работы оборудования, внедрение устройств перехвата информации в рабочих помещениях. Для уничтожения информационной базы возможно использовать простейшие воздействия: пожар или залив оборудования водой. При этом не обязательно воздействовать на помещение и оборудование, где хранится информация. Достаточно, например, организовать пожар в соседнем помещении, куда доступ посторонних значительно упрощен. Менее очевидными являются организационно-правовые способы воздействия угроз. К этим способам воздействия относится невыполнение персоналом и руководством требований нормативных документов, задержка с принятием нормативно-правовых положений. Невыполнение нормативных требований или их отсутствие часто открывают путь другим способам воздействия угроз. Угрозу могут представлять и действия, связанные с закупкой устаревшего оборудования, неправомерного ограничения доступа к информации и другие.

Предотвращение, парирование или нейтрализация угроз информационной безопасности осуществляется с помощью средств защиты информации на основании разработанных и внедренных методов противодействия различным угрозам информационной безопасности. Под средствами защиты информации понимаются организационные, технические, криптографические, программные средства, предназначенные для защиты информации с ограниченным доступом, а также программные средства и вычислительная техника, в которых они реализованы. Кроме того, к ним же относятся и средства контроля эффективности защиты информации.

Для эффективной и всесторонней защиты информации от существующих угроз необходимо использовать различные методы противодействия этим угрозам и предотвращения самой возможности их применения. Методы предотвращения, парирования или нейтрализации угроз можно разделить на организационно-правовые, меры физической защиты и программно-технические методы.

Организационно-правовые методы, прежде всего, включают в себя разработку комплекса нормативно-правовых актов и положе-

ний, регламентирующих информационные отношения, руководящих и нормативно-методических документов по обеспечению информационной безопасности. На основании этих нормативных документов создается система лицензирования деятельности в сфере информационной безопасности и стандартизация способов и средств защиты информации. В свою очередь, в организациях необходимо сформировать и обеспечить функционирование систем защиты секретной и конфиденциальной информации. Необходима сертификация и аттестация этих систем по требованиям руководящих документов в области информационной безопасности. При разработке АС одной из важнейших процедур является выработка должностных инструкций и регламентов поведения персонала в различных ситуациях. В процессе эксплуатации необходимо добиваться неуклонного выполнения этих инструкций.

Необходимо организовывать физическую защиту помещений, линий связи, каналов передачи информации, носителей информации с целью предотвращения физического проникновения, хищения или перехвата информации. Средства физической защиты весьма действенны при обеспечении информационной безопасности. Например, при рассмотрении вопросов классификации компьютеризированных СУиК ЯМ мы увидим, что именно наличие физической защиты позволяет использовать для целей учета ЯМ базовое программное обеспечение, сертифицированное по третьему классу безопасности от несанкционированного доступа.

И, наконец, непосредственно при проектировании и создании компьютерных сетей необходимо применять программно-технические методы противодействия угрозам информационной безопасности. В документе Гостехкомиссии России (в настоящее время ФСТЭК – Федеральная служба по техническому и экспортному контролю РФ) «Специальные требования и рекомендации по технической защите конфиденциальной информации» указано, что защита информационной среды достигается выполнением мероприятий и применением (при необходимости) средств защиты информации по предотвращению утечки информации или воздействия на нее по техническим каналам за счет несанкционированного доступа к ней, по предупреждению преднамеренных программно-технических воздействий с целью нарушения целостности (уничтожения, искажения) информации в процессе ее обработки, пере-

дачи и хранения, нарушения ее доступности и работоспособности технических средств. Особенно возрастает роль этих мероприятий при использовании открытых каналов передачи информации.

Кратко можно перечислить следующие меры:

• исключение несанкционированного доступа к информации, предотвращение специальных воздействий, вызывающих разрушение, уничтожение, искажение информации или сбои в работе средств информатизации;

• выявление внедренных программных или аппаратных закладных устройств;

• применение средств защиты от утечек информации по техническим каналам;

• применение средств защиты информации, в том числе криптографических, при передаче по каналам связи.

При планировании противодействий целенаправленным угрозам информационной безопасности следует учитывать, что хотя атаки извне на компьютерные системы широко обсуждаются и вызывают повышенное внимание, однако значительно больший ущерб безопасности вызывают внутренние нарушения безопасности. Требования информационной безопасности затрагивают интересы практически всех работников предприятия. Ситуация осложняется тем, что, наряду со своими основными обязанностями, эти работники должны выполнять зачастую непонятные и поэтому часто отторгаемые функции и процедуры, связанные с выполнением требований безопасности. Причинами этого может являться низкая квалификация персонала, недостаточная для корректной работы с АС, или халатность. Особо опасными являются некомпетентные сотрудники, выдающие себя за грамотных пользователей или считающие себя таковыми. При отсутствии в организации контроля за установкой на рабочих местах программного обеспечения сотрудник может установить на своём рабочем месте заинтересовавшую его программу, даже не понимая возможных последствий. Подобная угроза возникает и в случае подключения находящейся в локальной сети рабочей станции к сети Интернет через модем или мобильный телефон, оснащённый функцией цифровой связи. Угрозу представляет практика обмена паролями между работниками, выполняющими сходные функции, или оставление записанных паролей на рабочих местах. Очевидно, что данные проблемы нераз-

решимы только технологическими мерами, и вполне естественно, что меры безопасности объективно затрудняют выполнение сотрудниками своей работы. Например, специалисты по ИБ считают, что уменьшение срока действия паролей (вплоть до одноразового использования) существенно снижает риск их компрометации, однако такой прием может вызывать раздражение даже у высокодисциплинированных сотрудников. В таких случаях более эффективным является обучение, повышение бдительности сотрудников, то есть создание в организации «культуры информационной безопасности». Повсеместное распространение мобильных накопителей информации, таких, как flash-диски, винчестеры с USB-интерфейсом и т.д. обусловило появление нового класса угроз информационной безопасности. Проблема несанкционированного использования таких устройств невнимательными сотрудниками не всегда может быть решена мерами организационной защиты информации и также может привести к утечке информации. Единственной альтернативой физическому отключению USB-портов на рабочих местах может быть только использование специальной системы защиты.

Отдельные компьютеры, даже не включенные в локальную сеть, требуют соблюдения особых правил безопасности, если на них обрабатываются конфиденциальные сведения. Для защиты локальных (автономных) компьютеров от несанкционированного доступа и должны применяться и организационные и технические меры, реализующие четкий регламент обработки конфиденциальной информации. Средствами реализации технических мер являются средства аутентификации пользователя, шифрования в файловой системе, программно-аппаратные комплексы защиты информации от НСД.

3. ПРОБЛЕМЫ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ В СФЕРЕ УЧЕТА И КОНТРОЛЯ ЯДЕРНЫХ МАТЕРИАЛОВ

Прогресс в сфере вычислительной техники сопровождается бурным развитием программного обеспечения. Зачастую вновь созданные и распространяемые программные средства не отвечают современным требованиям безопасности. Примером может являться программное обеспечение, создаваемое наиболее мощной кор-

порацией в этой сфере деятельности – Microsoft. Выпускаемые операционные системы (ОС), системы управления базами данных (СУБД) содержат изъяны в обеспечении информационной безопасности и большое число «недокументированных возможностей». Их наличие позволяет злоумышленникам через глобальные сети внедряться в информационные системы, определять пароли пользователей, произвольно назначать себе уровни доступа и, в конечном итоге, свободно манипулировать конфиденциальной информацией.

Отставание теоретической проработки информационной безопасности от технологического прогресса и постоянно обновляющихся угроз безопасности приводит к тому, что большинство систем защиты занимается «латанием дыр», обнаруженных в процессе эксплуатации.

На ситуацию с обеспечением компьютерной безопасности существенное влияние оказывает тот факт, что существующие национальные стандарты в сфере информационной безопасности также отстают от требований, предъявляемых к безопасности современных информационных технологий. Глобализация информационного пространства привела к необходимости выработки международных критериев безопасности, которые должны стандартизировать требования к безопасности, обоснования применения тех или иных средств обеспечения информационной безопасности и корректность реализации средств защиты.

Надо отметить, что перечисленные проблемы осознаются и органами государственного управления и разработчиками систем вычислительной техники и программного обеспечения. В последнее время усилия по обеспечению защиты информации ставятся на первый план и при продвижении нового программного обеспечения. Созданы международные критерии обеспечения компьютерной безопасности, которые утверждены Международной организацией по стандартизации (ISO) в 1999 г. [6]. С 1 января 2004 г. этот стандарт действует и в Российской Федерации. Разработчики программного обеспечения стремятся сертифицировать свои продукты согласно этим критериям, что в целом должно поднять уровень обеспечения информационной безопасности. Так в 2002 году на соответствие этим критериям была сертифицирована операционная система Windows 2000, в 2003 году были сертифицированы некоторые дистрибутивы операционной системы Linux.

В Российской Федерации в целом тенденции развития информационных технологий в области обеспечения безопасности соответствуют общемировым. Тем не менее существуют и определенные особенности. Распространение информационных технологий в России несколько отстает от экономически развитых стран мира. С одной стороны это объясняется тем, что наша страна позднее развитых стран получила возможность развивать общедоступные информационные системы, с другой стороны экономическая ситуация в стране не позволяет сделать информационные технологии доступными большинству населения. Это отставание сказывается, например, в динамике развития нормативных документов в сфере информационной безопасности. Так, первые руководящие документы Гостехкомиссии России (ФСТЭК) [9–12] в сфере защиты информации от несанкционированного доступа были приняты в 1992 г. Идеология, отраженная в этих документах, соответствовала образцам критериев Министерства обороны США, так называемой «Оранжевой книги», принятых в 1983 г. Близок к этим документам и руководящий документ, регулирующий защиту информации в автоматизированных системах учета и контроля ядерных материалов [11], принятый в 1997 г. И только в 2004 г. в России стали стандартом Международные критерии.

На отечественном рынке практически отсутствуют специализированные средства работы с секретной информацией, такие, как операционные системы и СУБД. То, что используется в качестве базового программного обеспечения (ПО), не выдерживает критики с точки зрения обеспечения безопасности. Зачастую используются коммерческие системы, предназначенные для обеспечения работы малых предприятий и офисов и не ориентированные в принципе на работу с секретной информацией. Существующие средства защиты решают отдельные задачи, например задачу криптографии, но не в состоянии решить проблему в целом.

Если говорить о положении защиты информации в сфере учета и контроля ядерных материалов, то следует отметить, что использование коммерческого базового программного обеспечения, разработанного в третьих странах, для обработки информации, составляющей государственную тайну, едва ли может считаться нормальным. В аналогичных ситуациях правительства многих стран отказываются от импортного программного обеспечения и разраба-

тывают собственное ПО. Один из последних примеров такого рода – отказ ряда стран от использования программного обеспечения корпорации Microsoft для задач государственного и регионального управления. Существуют два пути решения этой проблемы [12]. Первый путь – это создание собственного программного обеспечения на отечественной платформе. Второй путь – доработка существующего ПО, заключается в создании собственных систем защиты информации (СЗИ) и внедрении их в существующие системы на основании лицензионных соглашений. Первый путь является очень затратным, и в настоящее время Росатом двигается по второму пути. В 2003 г. в рамках программы GSP (Government Security Program) корпорацией Microsoft предоставлена возможность ознакомления с исходными текстами своих операционных систем для уполномоченных организаций ряда стран. В России такое соглашение было подписано между корпорацией и ФАПСИ (позднее ФАПСИ было упразднено, а функции агенства переданы ФСБ). Заявлено также, что корпорация Microsoft будет предоставлять в установленном порядке для проведения оценки необходимую проектную документацию, а также возможность разработки программных модулей в тех случаях, когда предъявляемые функциональные требования не реализованы в продуктах корпорации Microsoft.

4. ПРОБЛЕМЫ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ В СФЕРЕ СИСТЕМ ФИЗИЧЕСКОЙ ЗАЩИТЫ

В отличие от систем учета и контроля, где обработка информации является одной из основных функций, в системах физической защиты это не совсем так. Физическая защита как составная часть системы по обеспечению сохранности ЯМ представляет собой целый комплекс организационных мероприятий, инженерно-технических средств и действий подразделений охраны в целях предотвращений диверсий или хищений. На практике он включает в себя несколько подсистем, каждая из которых должна обеспечивать эффективную защиту от угроз в ограниченной области. Согласно «Правилам физической защиты ядерных материалов, ядерных установок и пунктов хранения ядерных материалов» [3] подсистема

защиты информации должна входить в состав технических средств СФЗ наравне с другими подсистемами, такими как, СКУД, ОС. При автономном функционировании (то есть при отсутствии единого компьютеризированного центра сбора и обработки информации) каждая из этих подсистем может иметь собственные коммуникации, центры управления, причем информация может не представляться в цифровом виде. Например, состояние датчиков охраны отображается световой индикацией на сигнальных панелях, изображение с видеокамер выводится прямо на мониторы и т.п. Основные проблемы для информации такого типа лежат в области внешних физических воздействий: это повреждения коммуникаций, взаимные электромагнитные наводки или внешние помехи. Они рассматриваются с точки зрения надежности функционирования инженерно-технического комплекса и должны быть учтены при проектировании СФЗ.

Развитие информатики и микропроцессорных средств в 1980–90-е годы стимулировало внедрение компьютерных технологий практически во все подсистемы безопасности. Однако следует отметить, что аппаратура уровня датчиков и исполнительных устройств обычно реализуется на специализированных контроллерах или микропроцессорах. Эти устройства не связаны непосредственно с управляющими компьютерами и для них нет необходимости использовать относительно медленную среду операционной системы Windows. Программное обеспечение для них создается производителем и их программирование («прошивка») осуществляется с помощью специализированных приборов. Поэтому угрозы ИБ на этом уровне, в их традиционном понимании, практически отсутствуют. Переход к компьютерной обработке информации с использованием общепринятой архитектуры и протоколов происходит на уровне автоматизированных рабочих мест (АРМ) персонала предприятия и служб безопасности. Растущие требования к эффективности служб безопасности и охраны приводят к широкому внедрению автоматизированного контроля и управления СФЗ. Например, широкое распространение электронных пропусков и современных средств аутентификации (особенно, биометрической) требует от подсистемы управления и контроля доступом высокой степени автоматизации. Расширение использования оптико-электронного (видео, телевизионного) наблюдения приводит к разрыву возмож-

ностей этой подсистемы и оператора – человек не способен долгое время внимательно наблюдать за множеством картинок или мониторов. На уровне взаимодействия персонала с системой необходим постоянный и «дружественный» контакт компьютера с человеком, так как работа с системой на этом уровне необходима для сотрудников самых различных служб объекта. Поэтому данный уровень чаще всего реализуется на базе привычной для человека графической среды Windows или подобной. Рабочие места операторов и персонала должны быть организованы в удобном для восприятия информации виде с использованием графических планов объекта, пиктограмм, с постоянным интерактивным отображением их состояния цветом, текстовыми комментариями и инструкциями оператору. Современные тенденции развития СФЗ для важных объектов лежат в области объединения различных подсистем в единый комплекс. Как правило, это происходит на основе общей компьютеризированной системы и специального программного обеспечения. Такой подход позволяет строить СФЗ с организацией автоматизированных алгоритмов реакции на события, синхронизацией баз данных и автоматизацией поиска нужных событий в одной подсистеме при известных входных событиях в другой. В таких системах возможна организация удобных рабочих мест, с привязкой состояния и управления работой к графическим планам объекта, что облегчает деятельность операторов, уменьшает время реакции и принятия решений.

Комплексная компьютеризированная система управления физической защитой объекта обычно создается на базе локальной сети, объединяющей серверы управления подсистемами, автоматизированные рабочие места и серверы баз данных. При этом такая АС является многопользовательской и содержит информацию различной степени конфиденциальности. Например, рабочее место сотрудника бюро пропусков должно обеспечивать доступ только к персональным данным сотрудников. А рабочее место оператора или дежурного охраны – к графическим планам объекта, с данными о расположении средств охранной сигнализации. В первом случае, информация может являться конфиденциальной, во втором – секретной. Персонал, работающий с данными, относится к разным подразделениям и имеет разные уровни допуска. Эти обстоятельст-

ва предъявляют повышенные требования к разграничению доступа использующих систему сотрудников.

Например, в одной из российских интегрированных систем физической защиты доступ регулируется на трех уровнях программного обеспечения:

• уровень 1 – средства разграничения доступа и управления привилегиями пользователей, встроенные в операционную систему (например, Windows NT или Unix);

• уровень 2 – средства ограничения доступа к информации и управления привилегиями с использованием возможностей системы управления базами данных (СУБД);

• уровень 3 – средства, встроенные в само программное обеспечение управляющее доступом и охранными средствами, позволяющие пользователям предоставлять различные привилегии, что даёт возможность гибко разграничить доступ между различными операторами и администраторами системы. Например, существует возможность установки разной видимости информации на специализированных рабочих местах, например с рабочего места администратора доступна вся информация о работнике, а с рабочего места оператора будут видны только фамилии, инициалы и фотографии владельцев карт доступа без указания их категорий, мест работы домашних адресов и т.п.

В соответствии с введенным в действие с июня 2008 г. документом Ростехнадзора РФ «Требования к системам физической защиты ядерных материалов, ядерных установок и пунктов хранения ядерных материалов» [4] как технические, так и программные средства систем ФЗ, используемые при обработке секретной информации, подлежат обязательной сертификации, которая проводится на соответствие требованиям безопасности информации. Созданные и реконструированные системы физической защиты подлежат аттестации по требованиям безопасности информации. Требования к подобным АС формируются на базе руководящего документа Гостехкомиссии РФ «Автоматизированные системы. Защита от несанкционированного доступа к информации. Классификация автоматизированных систем и требования по защите информации» [8], выпущенного в 1992 г. Этот документ позже послужил основой и для формирования требований к компьютеризированным СУиК ЯМ. Следует отметить, что данный документ тре-

бует использовать для обработки и хранения секретной информации только сертифицированные средства вычислительной техники. Таким образом, используемые компьютеры и серверы должны быть аттестованы на соответствие требованиям защищенности от несанкционированного доступа (НСД).

5. СТАНДАРТЫ И НОРМАТИВЫ В СФЕРЕ ОБЕСПЕЧЕНИЯ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ В АВТОМАТИЗИРОВАННЫХ СИСТЕМАХ УИК И ФЗ ЯМ

Существует достаточно большой перечень документов Росатома, касающихся обеспечения информационной безопасности в автоматизированных системах предприятий и организаций министерства. Их перечень приводится в отраслевом стандарте по оснащению систем учета и контроля ядерных материалов [1]. Сам отраслевой стандарт содержит разделы, посвященные обеспечению информационной безопасности как с точки зрения защиты от НСД, так и с точки зрения надежности хранения информации. В данном разделе мы рассмотрим отечественные нормативные акты и документы в сфере защиты от НСД, которыми разработчики АС должны руководствоваться при создании средств защиты информации. Основным документом, устанавливающим классификацию СУиК ЯМ и регламентирующим требования по защите от НСД к информации в СУиК, является руководящий документ Гостехкомиссии РФ и Минатома «Требования по защите от несанкционированного доступа к информации в автоматизированных системах учета и контроля ядерных материалов», утвержденный в январе 1997 г. [11]. Этот документ содержит также требования по сертификации средств защиты информации в таких системах и аттестационные требования к АСУиК ЯМ. Данный документ при разработке учитывал руководящие документы Гостехкомиссии России в сфере информационной безопасности, выпущенные в 1992 г., и которые будут рассмотрены ниже. Существуют прецеденты, когда компьютеризированные СУиК ЯМ аттестовывались на основании именно этих критериев, а не на основании требований 1997 г.

Документом, в котором явно упомянуты требования по защите информации при разработке и эксплуатации компьютеризирован-

ных систем для управления ФЗ объекта, на котором используются или хранятся ЯМ, являются «Требования к системам физической защиты…» [4]. Фактически, в нем требуются сертификация и аттестация программных средств и аппаратной части, что приводит к необходимости применения действующих руководящих документов ФСТЭК.

5.1. Руководящие документы ФСТЭК России

В 1992 г. ФСТЭК России (тогда Гостехкомиссия РФ) опубликовала пять Руководящих документов, посвященных вопросам защиты от несанкционированного доступа к информации [6 - 10]. Эти документы послужили основой тех требований к СУиК ЯМ, которые мы рассмотрели выше. Поэтому кратко рассмотрим важнейшие их них.

Идейной основой этих документов является «Концепция защиты средств вычислительной техники от несанкционированного доступа к информации (НСД)» [6], содержащая систему взглядов ФСТЭК на проблему информационной безопасности и основные принципы защиты компьютерных систем. С точки зрения разработчиков данных документов основная задача средств безопасности заключается в обеспечении защиты от несанкционированного доступа к информации. Практически не рассматриваются вопросы поддержки работоспособности систем обработки информации. Этот уклон в сторону поддержания секретности объясняется тем, что эти документы были разработаны в расчете на применение в информационных системах министерства обороны и спецслужб РФ, а также невысоким уровнем информационных технологий начала 1990-х годов, по сравнению с современными.

Эти руководящие документы предлагают две группы критериев безопасности: показатели защищенности средств вычислительной техники (СВТ) от НСД и критерии защищенности автоматизированных систем обработки данных. Первая группа позволяет оценить степень защищенности отдельно поставляемых потребителю компонентов вычислительных систем, а вторая рассчитана на полнофункциональные системы обработки данных. Рассмотрим положения документа «Автоматизированные системы. Защита от не-

санкционированного доступа к информации. Классификация автоматизированных систем и требования по защите информации». Этот документ устанавливает классификацию автоматизированных систем по отношению к защищенности от НСД к информации. Имеет смысл сравнить эту классификацию с классификацией автоматизированных СУиК ЯМ.

Документы ФСТЭК устанавливают девять классов защищенности автоматизированных систем от НСД. Каждый из классов характеризуется определенной совокупностью требований к средствам защиты. В свою очередь классы подразделяются на три группы, отличающиеся спецификой обработки информации. Группа автоматизированной системы определяется на основании следующих признаков:

• наличие в АС информации различного уровня конфиденциальности;

• уровень полномочий пользователей АС на доступ к конфиденциальной информации;

• режим обработки данных в АС (коллективный или индивидуальный).

В пределах каждой группы устанавливается иерархия классов защищенности АС. Класс, соответствующий высшей степени защищенности для данной группы, обозначается буквой А, следующий класс обозначается Б и т.д.

Третья группа включает АС, в которых работает один пользователь, допущенный ко всей информации АС, размещенной на носителях одного уровня конфиденциальности. Группа содержит два класса – 3Б и 3А.

Вторая группа включает АС, в которых пользователи имеют одинаковые полномочия доступа ко всей информации, обрабатываемой и/или хранимой в АС на носителях различного уровня конфиденциальности. Группа содержит два класса - 2Б и 2А.

Первая группа включает многопользовательские АС, в которых одновременно обрабатывается и/или хранится информация разных уровней конфиденциальности. Не все пользователи имеют равные права доступа. Группа содержит пять классов - lД, 1Г, lВ, lБ и lА.

Анализ требований показывает, что второй класс защищенности от НСД к информации в компьютеризированных СУиК ЯМ в целом соответствует классу 1Б автоматизированных систем. Сущест-

вуют прецеденты, когда автоматизированная СУиК ЯМ, аттестованная по классу 1Б защищенности автоматизированных систем от НСД к информации используется для учета и контроля ЯМ в условиях, соответствующих второму классу СУиК ЯМ.

Разработка перечисленных документов в начале 90-х годов заполнила правовой вакуум в области стандартов информационной безопасности. Являясь, по сути, первым опытом стандартизации в столь деликатной сфере эти документы не лишены недостатков. Кроме того, за прошедшее с момента принятия этих критериев время получили развитие как теория информационной безопасности, так и подходы к формированию стандартов в сфере информационной безопасности. Главные недостатки реализованных в документах подходов заключается в том, что ранжирование требований по классу защищенности сводится к определению наличия определенного набора механизмов защиты, что существенно снижает гибкость и применимость данных требований на практике. Понятие политики безопасности в данных документов трактуется как поддержание режима секретности и отсутствия НСД. Из-за такого подхода средства защиты ориентируются исключительно на противодействие внешним угрозам, а к функционированию системы и ее структуре требований практически не предъявляется. Следует заметить, что требования к компьютеризированным СУиК ЯМ, принятые в 1997 году, созданы на основании перечисленных документов и сохраняют те же недостатки.

Требования по защите от НСД к информации в автоматизированных СУиК ЯМ

При разработке и эксплуатации компьютеризированных СУиК ЯМ необходимо руководствоваться документом «Требования по защите от несанкционированного доступа к информации в автоматизированных системах учета и контроля ядерных материалов»[11], выпущенным в 1997 г. совместно Минатомом и Гостехкомиссией РФ. Данный документ разработан Российским федеральным ядерным центром – ВНИИ экспериментальной физики (РФЯЦ ВНИИЭФ) и Тихоокеанской северо-западной национальной лабораторией (PNNL) США в рамках соглашения по модернизации

физической защиты, учета и контроля ядерных материалов в Российской Федерации. Основной целью данного документа являлась создание нормативной основы для сертификации по требованиям безопасности информации программного обеспечения автоматизированных СУиК ЯМ, разрабатываемого на базе коммерческих программных продуктов корпорации Microsoft. Документ вводит классификацию автоматизированных СУиК ЯМ, определяет требования с СЗИ от НСД к информации в зависимости от класса АСУиК и, наконец, определяет сертификационные и аттестационные требования средств защиты информации.

Классификация СУиК ЯМ

Классификация СУиК ЯМ вводится в целях разработки и применения обоснованных мер по достижению требуемого уровня защиты информации. Выбор класса защищенности производят заказчик и разработчик СУиК с привлечением специалистов в сфере защиты информации. В качестве критериев при установлении класса защищенности используются следующие свойства системы:

- наличие в СУиК информации различной степени секретности;
- уровень полномочий пользователей на доступ к секретной информации;
- порядок и условия размещения и функционирования, физическая защищенность средств вычислительной техники СУиК.

Исходя из оценки этих факторов, требования устанавливают три класса защищенности автоматизированных СУиК ЯМ. Самым высоким является первый класс.

К *третьему классу* относятся СУиК, если в них:

- имеется информация строго одной степени секретности;
- все субъекты доступа (кроме администраторов) имеют равные права доступа (полномочия) ко всей информации СУиК;
- все средства вычислительной техники СУиК размещаются в контролируемой зоне и не имеют внешних (выходящих за пределы контролируемой зоны) физических информационных связей.

Ко *второму классу* относятся СУиК, если в них:

- имеется информация нескольких степеней секретности;
- субъекты доступа имеют разные права доступа к информации СУиК;

• все средства вычислительной техники СУиК размещаются в пределах одной или нескольких контролируемых зон и не имеют незащищенных внешних физических информационных связей.

К *первому классу* относятся СУиК, если в них:

• имеется информация нескольких степеней секретности;

• субъекты доступа имеют разные права доступа к информации СУиК;

• средства вычислительной техники СУиК размещаются в контролируемой зоне и имеют внешние физические информационные связи со средствами вычислительной техники, не относящимися к СУиК.

В настоящее время все сертифицированное базовое программное обеспечение относится только к третьему классу. В табл. 5.1 приведены программные продукты, сертифицированные для использования в компьютеризированных СУиК ЯМ. Сертификаты на эти продукты продлены до 2009 г.

Таблица 5.1

Базовое программное обеспечение, сертифицированное для использования в компьютеризированных СУ и К ЯМ

Тип программного обеспечения	Наименование
Операционные системы	MS Windows NT 4.0 Workstation (Russian) с пакетом обновления SP 3 или SP 5
	MS Windows NT 4.0 Server с пакетом обновления SP 3 или SP 5
	MS Windows NT 4.0 Server Enterprise Edition с пакетом обновления SP 5
Системы управления базами данных (СУБД)	Microsoft SQL Server версии 6.5. с пакетом обновления SP 4 или SP 5a
	Oracle7 Server и Workgroup Server версии 7.3.4.0.0
	Oracle8i Enterprise Edition версии 8.1.7.0.0

На нынешнем этапе развития Федеральной информационной системы отсутствие базового программного обеспечения, сертифицированного на класс выше третьего, представляет собой основную проблему, сдерживающую развитие компьютеризированного учета. Принадлежность СУиК к третьему классу предполагает наличие информации одной степени секретности. Вместе с тем на предприятиях отрасли часто используются материалы, имеющие различный

уровень секретности. В этом случае выполнение требований Гостехкомиссии должно сопровождаться либо созданием не менее двух не связанных между собой локальных компьютерных сетей для учета материалов с различной степенью секретности, либо автоматическим повышением уровня секретности всех материалов до максимального. В первом случае затраты на создание сети резко увеличиваются, во втором – серьезно затрудняется работа персонала с материалами, изначально обладающими низким уровнем секретности. Наконец, последнее требование предполагает, что все предприятие размещено на одной площадке. Для крупных предприятий топливного цикла это требование не выполняется. Единственный выход в этом случае – создание фрагментов компьютеризированной системы на отдельных площадках и организация связи между ними посредством пересылки информации на носителях со специальными курьерами.

Таким образом, актуальной задачей является сертификации базового ПО по второму классу защиты информации от НСД. СУиК первого класса защищенности потребуются в том случае, когда возникнет потребность в передаче информации по открытым информационным каналам.

Требования к СЗИ от НСД к информации по классам СУиК

Требования Гостехкомиссии выделяют четыре подсистемы Системы защиты информации от несанкционированного доступа (СЗИ НСД). Это подсистемы:

- управления доступом к информации;
- регистрации и учета;
- криптографическая;
- обеспечения целостности.

К каждой подсистеме, в зависимости от класса СУиК, устанавливаются сертификационные и аттестационные требования.

Под сертификацией СЗИ понимается установление соответствия средств защиты информации набору требований, обеспечивающих защиту сведений соответствующей степени секретности. Порядок проведения обязательной сертификации СЗИ и организации, уполномоченные проводить сертификацию, подробно описаны в разделе «Разработка и ввод в эксплуатацию компьютеризированных

СУиК ЯМ». В настоящем разделе приводятся сертификационные требования к различным подсистемам СУиК в зависимости от ее класса. Требования к более высокому классу автоматически включают в себя требования к более низкому классу.

Далее приводятся требования к *СУиК третьего класса*. К компонентам *подсистемы управления доступом* предъявляются требования, в соответствии с которыми должны осуществляться:

• идентификация и аутентификация пользователей при входе в операционную систему;

• идентификация и аутентификация пользователей при доступе к системе управления базами данных (СУБД);

• идентификация серверов, рабочих станций, внешних и сетевых устройств по физическим адресам;

• идентификация субъектов и объектов по именам;

• идентификация объектов баз данных по именам.

К компонентам *подсистемы регистрации и учета* предъявляются следующие требования. Должна осуществляться регистрация следующих событий:

• входа/выхода пользователей в операционную систему/из системы, а также регистрация загрузки операционной системы и ее программного останова;

• запуска/завершения всех программ;

• попыток доступа программных средств к защищаемым файлам и каталогам;

• доступа к объектам базы данных.

Средства регистрации должны быть доступны только администратору и включать для него средства для просмотра и анализа накапливаемых событий по указанным параметрам и их архивирования.

При регистрации должны указываться:

• время и дата процесса входа/выхода пользователя в систему/из системы, загрузки/останова системы;

• идентификатор пользователя, инициализирующего процесс;

• результат действия (успешное или неуспешное – несанкционированное).

При доступе к файлам или объектам базы данных регистрируется также спецификация объекта доступа и код запрашиваемой операции.

Подсистема обеспечения целостности должна обеспечивать:

• целостность программных средств и информационной базы СЗИ НСД.

• целостность информационной базы СЗИ НСД в СУБД посредством ее изолирования от пользователей и оперативного восстановления со стороны администратора.

Криптографическая система у СУиК третьего класса отсутствует.

Далее приводятся требования к *СУиК второго класса*. Подсистема управления доступом должна осуществлять:

• идентификацию каналов связи по физическим адресам;

• контроль доступа субъектов к защищаемым ресурсам ОС в соответствии с матрицей доступа на основе дискреционного принципа;

• контроль доступа субъектов к объектам СУБД в соответствии с матрицей доступа по операциям выборки, модификации, вставки, удаления и т.п.;

• ограничение доступа пользователей к защищаемым объектам только с помощью строго установленных процессов;

• мандатный принцип управления доступом;

• управление потоками информации с помощью атрибута секретности субъектов и объектов;

• передача данных по сети должна осуществляться вместе с атрибутами секретности, которые должны быть защищены.

Несанкционированные действия над передаваемыми по сети данными и несанкционированное дублирование данных должны надежно идентифицироваться как ошибка с соответствующей регистрацией.

Принципы управления доступом к объектам будут излагаться в главе 3.

При передаче данных по сети требования Гостехкомиссии устанавливают, что должны использоваться средства, предотвращающие передачу данных объекту, имеющему степень секретности ниже, чем передаваемые данные.

Подсистема регистрации и учета должна осуществлять:

• регистрацию выдачи секретных печатных документов на «твердую» копию;

• регистрацию попыток доступа программных средств к следующим защищаемым объектам доступа: узлам и фрагментам сети, портам, внешним устройствам, процессам;

• регистрацию всех выявленных ошибок при обмене данных по сети;

• автоматический учет создаваемых защищаемых объектов с помощью их дополнительной маркировки, используемой в подсистеме управления доступом;

• очистку (обнуление, инициализация, обезличивание) освобождаемых областей ОЗУ ЭВМ и разделяемых внешних накопителей. Очистка осуществляется двукратной произвольной записью в любую освобождаемую область памяти, использованную для хранения защищаемой информации.

При выдаче на печать секретных документов необходимо осуществлять автоматическую маркировку листов номерами и учетными реквизитами. Одновременно должна оформляться учетная карточка документа с определенными параметрами регистрации.

Требования к подсистемам обеспечения целостности и криптографии полностью совпадают с требованиями к аналогичным подсистемам СУиК третьего класса.

Требования к *СУиК первого класса* полностью включают в себя требования к СУиК третьего и второго класса.

Требования к *подсистеме управления доступом* включают в себя аутентификацию пользователей при удаленном доступе к серверу, рабочей станции с помощью методов, устойчивых к прослушиванию каналов и активному воздействию на передаваемые в сети данные. Также должна проводиться аутентификация субъекта-источника данных, т.е. должны использоваться средства, подтверждающие подлинность источника блока данных с помощью методов, устойчивых к прослушиванию каналов и активному воздействию на передаваемые данные в сети.

Подсистема регистрации и учета должна осуществлять регистрацию изменения полномочий субъектов доступа и статуса объектов доступа. Должна так же осуществляться регистрация установления соединения между удаленными процессами и сигнализация попыток нарушения защиты на дисплей рабочей станции администратора и нарушителя.

Криптографическая подсистема должна осуществлять шифрование всей секретной информации, записываемой на совместно используемые различными субъектами доступа носители данных, в каналах связи сети, а также на съемные носители данных. Доступ субъектов к операциям шифрования и к соответствующим криптографическим ключам должен дополнительно контролироваться посредством подсистемы управления доступом.

Подсистема обеспечения целостности должна обеспечивать:

• целостность соединения для защиты передаваемых по сети данных пользователя от несанкционированной модификации, подстановки или изъятия любых данных с помощью методов, устойчивых к прослушиванию каналов и воздействию на передаваемые данные в сети;

• доказательство источника данных с целью предотвращения любой попытки отправителя данных отрицать впоследствии факт передачи;

• доказательство доставки данных для предотвращения любой попытки получателя данных отрицать впоследствии факт получения данных.

Требования по аттестации СЗИ от НСД по классам СУиК ЯМ

Аттестации подлежит вся компьютеризированная СУиК ЯМ. Под аттестацией понимается документированное подтверждение соответствия применяемого при эксплуатации комплекса организационно-технических мероприятий требованиям стандартов и иных нормативных документов по безопасности информации. Предусматривает аттестационные испытания защищаемой АС в условиях эксплуатации для оценки соответствия используемых мер и СЗИ требуемому уровню безопасности информации. Далее информация располагается в том же порядке, что и требования по сертификации.

Далее приводятся требования к *СУиК третьего класса*. К компонентам *подсистемы управления доступом* предъявляются следующее аттестационное требование. Доступ персонала к информации СУиК должен осуществляться в соответствии с действующей разрешительной системой допуска исполнителей к секретным документам и сведениям.

Подсистема регистрации и учета должна:

• проводить учет всех защищаемых носителей информации с помощью их любой маркировки;

• регистрировать и учитывать выходные печатные документы ручным способом в соответствии с требованиями делопроизводства соответствующей степени секретности. Выдача печатных документов должна осуществляться только в соответствии с установленным перечнем выходных документов с указанием их степени секретности.

Подсистема обеспечения целостности должна обеспечивать следующий набор функций:

• должна быть обеспечена неизменность программной среды, при этом целостность программной среды обеспечивается отсутствием в СУиК средств разработки и отладки программ;

• должно проводиться периодическое тестирование функций СЗИ НСД при изменении программной среды и персонала СУиК с помощью тестов, имитирующих попытки НСД;

• должны быть в наличии средства восстановления СЗИ НСД, предусматривающие ведение двух копий программных средств СЗИ НСД и их периодическое обновление и контроль работоспособности, а также оперативное восстановление функций СЗИ НСД при сбоях аппаратуры;

• помещения с техническими средствами СУиК, на носителях которых содержится секретная информация, должны быть оборудованы техническими средствами охраны, обеспечивающими уровень защиты, соответствующий степени секретности хранимой информации;

• должны использоваться средства защиты информации от НСД, сертифицированные для данного класса СУиК.

Аттестационные *требования к СУиК второго класса* отличаются от требований к СУиК третьего класса только в отношении *подсистемы обеспечения целостности*. Должен быть предусмотрен администратор защиты информации, ответственный за ведение, нормальное функционирование и контроль работы СЗИ НСД. Администратор должен иметь свою рабочую станцию и необходимые средства оперативного контроля и воздействия на безопасность СУиК. Кроме того, должны использоваться защищенные линии связи, выходящие за пределы контролируемых зон.

Аттестационные *требования к СУиК первого класса* отличаются от требований к СУиК второго класса наличием *криптографической подсистемы*. Должны использоваться криптографические средства, сертифицированные для СУиК первого класса. Кроме того, *подсистема обеспечения целостности* должна использовать межсетевые экраны, сертифицированные для СУиК первого класса

5.2. Общие критерии безопасности информационных технологий

«Общие критерии» (Common Criteria for Technology Security Evaluation) представляют собой результат последовательных усилий по разработке критериев оценки безопасности информационных технологий, которые были бы приняты в качестве Международных критериев.

В начале 1980-х годов в США были разработаны «Критерии оценки доверенных компьютерных систем». В следующем десятилетии различные страны проявили инициативу по разработке критериев оценки, которые строились на концепциях этого документа, но были бы более гибки и адаптируемы к развитию информационных технологий.

Так в 1991г. Европейской комиссией были опубликованы «Критерии оценки безопасности информационных технологий», разработанные совместно Францией, Германией, Нидерландами и Великобританией. В Канаде в начале 1993 г. были созданы «Канадские критерии оценки доверенных компьютерных продуктов». В США в это же время был издан проект стандарта «Федеральные критерии безопасности информационных технологий».

В 1990 г. Международной организацией по стандартизации (ISO) была начата разработка международного стандарта критериев оценки для общего использования. Новые критерии были призваны удовлетворить потребность взаимного признания результатов стандартизированной оценки безопасности на мировом рынке информационных технологий. В июне 1993 г. организации, разработчики национальных критериев, объединили свои усилия и начали действовать совместно, чтобы согласовать различающиеся между собой критерии и создать единую совокупность критериев безопасности.

Первая версия Общих критериев была завершена в январе 1996 г. и одобрена ISO в апреле 1996 г. для распространения в качестве проекта комитета. Был проведен ряд экспериментальных оценок, а также организовано широкое публичное обсуждение документа. Затем в рамках проекта Общих критериев была предпринята значительная переработка документа на основе замечаний, полученных при его экспериментальном использовании. Вторая версия вышла в мае 1998 года. Версия 2.1 этого стандарта утверждена ISO в 1999 году в качестве международного стандарта информационной безопасности ISO/IEC 15408. Сейчас в ряде стран наличие сертификата СС обязательно для информационных систем, важных с точки зрения национальной безопасности.

27 марта 2003 года ФСТЭК России представил план работ по внедрению международного стандарта в области информационной безопасности. Россия стала внедрять международный стандарт практически без изменений, разделив его на три ГОСТа под одним номером ИСО/МЭК 15408-2002. Серия новых ГОСТов вступила в действие в России с 1 января 2004 года.

Кратко ознакомимся с новым стандартом. Сам стандарт достаточно сложен и объемен. Он состоит из трех частей общим объемом около 600 страниц.

Часть 1 стандарта содержит методологию оценки безопасности ИТ, определяет виды требований безопасности (функциональные и доверия), основные конструкции (профиль защиты, задание по безопасности) представления требований безопасности в интересах трех категорий пользователей: потребителей, разработчиков и оценщиков продуктов и систем ИТ. Требования безопасности объекта оценки (ОО) по методологии Общих критериев определяются исходя из целей безопасности, которые, в свою очередь, основываются на анализе защищаемых информационных ресурсов, назначения ОО и условий среды его использования (угроз, предположений, политики безопасности).

Часть 2 стандарта содержит универсальный систематизированный каталог функциональных требований безопасности и предусматривает возможность их детализации и расширения по определенным правилам.

Часть 3 стандарта содержит систематизированный каталог требований доверия, определяющих меры, которые должны быть при-

няты на всех этапах жизненного цикла продукта или системы ИТ для обеспечения уверенности в том, что они удовлетворяют предъявленным к ним функциональным требованиям безопасности. В этой же части содержатся оценочные уровни доверия, представляющие собой стандартизованные наборы требований, которые позволяют с возрастающей степенью полноты и строгости провести оценку проектной, тестовой и эксплуатационной документации, правильности функционирования комплекса средств безопасности, оценку уязвимостей продукта или системы ИТ, стойкости механизмов защиты.

Как следует из содержания, Общие критерии представляют собой методический документ, содержащий хорошо систематизированный и структурированный набор требований, формы их представления и методологию задания. С использованием этих критериев оценка безопасности проводится не по жесткой схеме и единому штампу для различных продуктов информационных технологий (ИТ), как это предусмотрено в действующих документах ФСТЭК России, а исходя из назначения, видов и условий применения продуктов и систем ИТ с возможностью гибкого подхода к формированию соответствующих требований безопасности в профилях защиты. Причем профили защиты, разрабатываемые на основе ОК, могут включать и любые другие обоснованные требования, необходимые для обеспечения безопасности конкретного типа изделий ИТ.

Как показывают оценки специалистов в области информационной безопасности, по уровню систематизации, полноте и возможностям детализации требований, универсальности и гибкости в применении Общие критерии представляют наиболее совершенный из существующих в настоящее время стандартов.

Следует отметить, что Международное соглашение распространяется только на признание результатов оценки продуктов и систем информационных технологий, предназначенных для обработки конфиденциальной информации (до уровня доверия EAL 4 включительно), и не затрагивает вопросов оценки продуктов и систем, предназначенных для обработки информации, составляющей государственную тайну стран-участниц Международного соглашения. В то же время, методология Общих критериев может быть использована заинтересованными сторонами и в этих интересах.

США с января 2001 г. полностью перешли на оценку безопасности ИТ по Общим критериям, в передовых странах Европы (ФРГ, Франции и др.) около 40% разработанных в последние годы продуктов ИТ оценивалось по Общим критериям, причем тенденция оценки вновь разрабатываемых продуктов – по Общим критериям.

Агентство национальной безопасности США выпустило в мае 2000 г. директиву №140-23 об использовании с июля 2002 г. Министерством обороны США, а также его контракторами, представляющими государственные организации или коммерческими компаниями, для обработки чувствительной информации только продуктов и систем информационных технологий, сертифицированных по Общим критериям.

Одновременно действие этой директивы распространяется на атомные станции, находящиеся в частном пользовании, поскольку в США придается особое внимание роли Общих критериев при оценке безопасности информационных технологий, используемых в критически важных системах.

Все это свидетельствует о внимании, уделяемым мировым сообществом проблемам информационной безопасности, и об интересе к решению этих проблем на основе подходов и методологии Общих критериев.

В рамках подготовки к введению в России нового стандарта специалисты Центра «Атомзащитаинформ», ЦНИИАТОМИНФОРМ и ЦБИ разработали Комментарии к российскому стандарту, предназначенные для лучшего понимания российскими специалистами назначения, основных концептуальных положений, методологии и терминологии Общих критериев, а также для пояснения расхождений в терминологии стандарта с принятой в России терминологией и действующими нормативными документами.

Основным сопутствующим документом, выпущенным в поддержку Общих критериев и являющимся обязательным для использования в рамках упомянутого Международного соглашения, является «Общая методологии оценки безопасности информационных технологий», перерабатываемая в настоящее время специалистами ряда стран-участников Международного соглашения. В настоящее время на основе аутентичного перевода актуальной версии Общей методологии коллективом специалистов ЦБИ, Центра «Атомзащитаинформ» и ЦНИИАТОМИНФОРМ при участии экспертов меж-

дународной рабочей группы по Общим критериям осуществляется разработка методологии оценки продуктов и систем ИТ.

По плану ввода в действие Стандарта разработаны:

Руководящий документ «Руководство по разработке профилей защиты и заданий по безопасности» [21];

Руководящий документ «Безопасность информационных технологий. Руководство по регистрации профилей защиты» [22] на основе Стандарта.

Помимо этого предусмотрено проведение ряда дополнительных мероприятий:

• создание инструментального комплекса автоматизации разработки профилей защиты и заданий по безопасности (находится в разработке ЦБИ);

• разработка профилей защиты основных типов продуктов и систем ИТ: операционных систем, систем управления базами данных, межсетевых экранов, виртуальных частных сетей и др. (в ряде организаций, среди них: ЦБИ, ЦНИИАТОМИНФОРМ, МИФИ, ведется разработка профилей защиты для продуктов и систем информационных технологий различного назначения, в частности, ЦНИИАТОМИНФОРМ разрабатывает профиль защиты по II классу защищенности для автоматизированных СУиК ЯМ);

• разработка типовых методик проведения сертификационных испытаний продуктов и систем ИТ на основе Общей методологии оценки;

• проведение сертификационных испытаний ряда продуктов и систем ИТ, в том числе операционных систем (в частности, семейства Windows).

Указанные мероприятия были направлены не только на внедрение ГОСТ Р ИСО/МЭК 15408-2002 «Критерии оценки безопасности информационных технологий», но и на последующее присоединение России к Международному соглашению в качестве участника, выдающего сертификаты по Общим критериям.

В Минатоме России, как упоминалось ранее, также рассматриваются вопросы оценки и сертификации по требованиям Общих критериев программных продуктов, используемых в СУиК ЯМ. Следует констатировать, что для этого необходимо разработать профиль защиты для систем III класса защищенности, а также задания по безопасности, на соответствие которым провести сертификацию выбранных для этих целей программных продуктов. От

решения этих вопросов будут зависеть совершенствование действующих и разработка новых СУиК ЯМ, равно как и функционирование Федеральной информационной системы учета и контроля ядерных материалов.

По мнению российских специалистов, участвующих в освоении методологии Общих критериев, ввод в действие Российского стандарта, Общей методологии оценки, иных нормативных и методических документов в их поддержку, а также практическая работа по использованию методологии Общих критериев позволяет:

• выйти на современный уровень критериальной и методической базы оценки безопасности информационных технологий;

• создать новое поколение межведомственных и ведомственных нормативных и методических документов по оценке безопасности ИТ на единой основе;

• заказчикам и разработчикам изделий информационных технологий иметь мощный инструмент определения требований к безопасности ИТ и создания систем защиты информации;

• потребителям объективно оценивать возможности ИТ-продуктов по защите информации;

• заказчикам и разработчикам автоматизированных систем различного уровня и назначения иметь возможность соответственно более обоснованно формулировать и реализовывать требования по безопасности информации этих систем;

• сделать реальной перспективу вхождения России в Международное соглашение, что в свою очередь даст возможность:

– заказчикам и разработчикам ИТ-систем сократить свои затраты на сертификацию продуктов;

– для потребителей расширить рынок сертифицированных продуктов;

– испытательным лабораториям привлечь дополнительный поток заказов на сертификацию из-за рубежа;

– производителям российских высокотехнологичных продуктов получить международные сертификаты в России, что позволит им выйти на закрытые ранее зарубежные рынки.

При этом Россия (как и другие страны, присоединившиеся к соглашению о взаимном признании сертификатов) сохраняет возможность учета своих национальных требований при сертификации продуктов и систем ИТ и, прежде всего, предназначенных для защиты информации, составляющей государственную тайну.

Вместе с тем на этом пути предстоит большой объем работ, связанных с освоением Общих критериев и Общей методологии оценки в практической деятельности по заданию требований и оценке безопасности информационных технологий, по приведению в соответствие с международными стандартами, в частности, со стандартом ИСО/МЭК 15408-99 российской терминологии и российских стандартов в области безопасности информационных технологий, с выходом российских испытательных лабораторий (центров) и органов по сертификации, а также российской продукции, сертифицированной в соответствии с методологией Общих критериев, на международный рынок продукции и услуг.

Для этого необходимо преодолеть ряд трудностей технического, организационного и финансового характера, связанных:

• для разработчиков ИТ-продуктов – с четким соблюдением предусмотренных процедур подготовки и представления для оценки свидетельств, сопровождением жизненного цикла изделий;

• для заказчиков и разработчиков автоматизированных систем – с разработкой или обоснованным выбором профилей защиты, заданий по безопасности и, соответственно, ИТ-продуктов, отвечающих реальным потребностям безопасности создаваемых автоматизированных систем;

• для испытательных центров и органов по сертификации – с подготовкой и приведением в соответствие международным стандартам их деятельности по оценке безопасности ИТ, а также их аккредитацией в рамках Международного соглашения.

Однако пройти этот путь необходимо. Это позволит использовать богатый опыт, накопленный до настоящего времени мировым сообществом не только в области стандартизации, но и в области развития ИТ в целом, даст возможность российским специалистам активно участвовать в создании новых и совершенствовании действующих международных стандартов, и таким образом влиять на ход развития ИТ и их безопасности.

Следует учитывать, что введение новых стандартов не отменяет требований, представленных в руководящих документах ФСТЭК РФ.

5.3. Влияние Федерального закона «О техническом регулировании» на обеспечение безопасности информационных технологий

1 июля 2003 года произошло еще одно событие, которое в перспективе окажет большое влияние на политику в области информационной безопасности. Вступил в действие Федеральный закон «О техническом регулировании». Этот закон регулирует отношения, возникающие при разработке, принятии, применении и исполнении обязательных требований к продукции, процессам производства, эксплуатации, хранения, перевозки, реализации и утилизации; разработке, принятии, применении и исполнении на добровольной основе требований к продукции, процессам производства, эксплуатации, хранения, перевозки, реализации и утилизации, выполнению работ или оказанию услуг. К сфере регулирования этого закона относятся и вопросы создания продукции и оказания услуг в сфере информационной безопасности [16, 17].

Новый закон призван упростить процедуры поступления товаров на рынок, создать предпосылки для гармонизации российской и международной систем стандартизации, ввести в рамки закона права контрольно-надзорных органов. Закон декларирует доступность стандартов для пользователей, возможность участия производителей и потребителей в выработке регламентов и стандартов. Закон предусматривает выработку технических регламентов, которые гарантируют безопасность товаров и услуг и будут обязательны для производителей. Стандарты же делаются необязательными к исполнению. Потребитель сам должен оценить качество продукции и отдать предпочтение более качественной, в частности, сертифицированной на соответствие тем или иным стандартам.

Вместе с тем такие глубокие изменения в сфере стандартизации создают определенные опасности. Среди них: необязательность следования стандартам со стороны производителей, возможное снижение качества продукции и отсутствие ответственности за него. В день вступления в силу нового закона в Москве состоялась конференция «IT-SECURITY: новые требования к участникам рынка информационной безопасности».

Отмечая положительные стороны принятия нового закона, участники дискуссий сформулировали конкретные предложения госу-

дарственным органам, направленные на исключение возможных негативных последствий законодательных реформ в сфере информационной безопасности. Перечислим основные предложения:

• сохранить на переходный период действующий в настоящее время порядок применения технических требований к средствам обеспечения информационной безопасности;

• внести в Закон изменения, направленные на разработку и ввод технических регламентов по информационной безопасности;

• назначить ответственный государственный орган за разработку технических регламентов в области информационной безопасности;

• исключить лицензирование использования любых средств защиты информации;

• совместить испытательные лаборатории и сертификационные центры различных ведомств в «одно окно»;

• определить право на защиту какого рода информации гарантирует государство, а когда заказчик и исполнитель вправе руководствоваться при определении качества услуг или продуктов любыми механизмами от корпоративных стандартов до экспертных оценок;

При выполнении этих рекомендаций, считают участники конференции, принятый закон послужит делу улучшения положения дел в сфере информационной безопасности. В любом случае, на протяжении переходного периода (в течение 7 лет) продолжают действовать все нормативные документы.

6. ВОПРОСЫ НАДЕЖНОСТИ АС И РЕЗЕРВИРОВАНИЕ ИНФОРМАЦИИ

Вопросы надежности и отказоустойчивости информационных систем наряду с вопросами обеспечения защиты информации от несанкционированного доступа являются определяющими в деле обеспечения информационной безопасности. Российские критерии информационной безопасности, как видно из материала рассмотренного ранее, основной упор ставят на противодействие субъективным угрозам безопасности. Тем не менее надежность систем

играет не меньшую роль в проблемах, с которыми сталкиваются при проектировании и эксплуатации АС в областях ФЗ и УиК ЯМ.

Немецкая страховая компания GERLIG приводит следующие данные [18]. В 74% случаев причиной прекращения деятельности предприятий в Германии стала именно утеря информации. Статистика показывает, что в случае остановки информационной системы существует критический срок восстановления работоспособности системы. Если в указанный срок восстановления информации не произошло, то со 100% вероятностью организация прекратит свое существование. Для страховой компании этот срок 5,5 дней, у производственного предприятия – 5, у банка – 2, у предприятия непрерывного производственного цикла – около суток.

При оценках такого рода необходимо учитывать, что работоспособность многих критических приложений должна быть обеспечена со стопроцентной гарантией, поскольку от их деятельность зависит инфраструктура всего современного общества (правоохранительные органы, органы государственной власти, энергогенерирующие и транспортные компании и т.п.). Предприятия, имеющие в обращении ядерные материалы, относятся к этим критическим системам. Полная потеря информации об ядерных материалах должна быть исключена со 100% гарантией. Стандарт отрасли [1] устанавливает некоторые требования и нормативы, связанные с обеспечением надежности СУиК ЯМ.

Система физической защиты ядерного объекта относится к системам класса 24.7.365 – должна работать 24 часа в сутки, семь дней в неделю, 365 дней в году. Исходя из этого к надежности программных и аппаратных комплексов для АС ФЗ предъявляются жесткие требования. Базы данных, используемые в компьютеризированных системах ФЗ, содержат, как правило, сведения о персонале (например, для системы контроля доступа), обширные архивы событий, видеоданных и конфигурацию системы. В силу требований режима секретности и учета кадров, большинство персональной информации дублировано на бумажных носителях, однако ее утеря в компьютеризированной системе приведет к существенному сбою в деятельности предприятия и резко снизит эффективность служб безопасности. Вся накопленная информация по событиям также будет утеряна. Современные подсистемы охранной сигнализации и контроля доступа максимально защищаются от физических воздей-

ствий, и сбоев в электрических сетях путем резервирования линий электропитания, использования внутренних аккумуляторов и накопителей. Управляющие контроллеры снабжаются собственной памятью, в которой, при временной потере связи с серверами, может долгое время накапливаться и храниться информация о событиях, зафиксированных подключенными датчиками или считывателями. Практически все производители закладывают возможность автоматической пересылки накопленных данных на центральный сервер при восстановлении связи.

Для исключения возможности полной потери информации в условиях нормальной эксплуатации и при проектных авариях необходимо предусматривать систему хранения и восстановления данных. Эта система включает в себя следующие элементы:

• 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 резервных копий, которые необходимо хранить отдельно либо в хранилище файлов, либо (и) по соответствующему соглашению в другом компьютерном центре.

Перечисленные пункты относятся к выбору стратегии резервирования функций и информации. Дадим некоторый комментарий указанным положениям. Как правило, в локальных сетях, предназначенных для обработки важной информации, необходимо предусматривать резервный сервер (резервный контроллер домена в сетях под управлением Windows NT). В процессе работы периодически осуществляется синхронизация данных главного и резервного серверов. В случае выхода из строя главного сервера обработка информации автоматически переводится на резервный. Современные решения предлагают различного рода кластерные системы с распределенной нагрузкой, когда выход из строя сервера не прекращает эксплуатации всей системы. Для систем управления физической защитой наиболее актуальна схема «горячего» резервирования, когда отказавший сервер автоматически заменяется резервным без участия оператора. Если система работает с несколькими базами данных, а компьютеры объединены в локальную сеть и проис-

ходит обрыв связи между данными компьютерами, то система распадается на независимые сегменты. Работу каждого из сегментов обеспечивает свой программный сервер со своей базой данных. Очевидно, что изначально базы данных содержат эквивалентную информацию. С течением времени в каждой из баз она будет изменяться произвольным образом. В итоге, когда связь между компьютерами будет восстановлена, в системе образуются разные базы данных, содержащие несовпадающую информацию. Эти базы необходимо синхронизировать. И в момент синхронизации данных возможны коллизии: если в обеих базах была изменена разным образом информация об одном и том же объекте, тогда, как правило, решение о том, какую версию данных использовать, принимается администратором системы. Существуют автоматические варианты разрешения подобных конфликтов: по приоритетам (принимается изменение того программного сервера, чей приоритет выше), по времени (чье изменение произошло позднее, то и принимается). Для повышения устойчивости АС к сбоям и обрывам связи может использоваться кольцевая топология локальной сети. В этом случае всегда существует возможность связи в обход нерабочего участка.

RAID-технология (Redundancy Array of Independent Disks) представляет собой использование вместо одного магнитного накопителя массива из многих, относительно недорогих, дисков с высокой надежностью и скоростью работы. Этот дисковый массив организуется с помощью контроллера таким образом, чтобы полученная система обладала большей надежностью, чем надежность составляющих его дисков. Используются различные режимы записи информации на диски, позволяющие зеркально дублировать информацию или восстанавливать ее после сбоев. Очень часто такие высоконадежные дисковые массивы объединяются для работы с кластерными системами. Однако следует понимать, что катастрофический отказ RAID-массивов приведет к полной остановке таких систем.

При выборе стратегии резервирования необходимо оценивать требования к системе в области поддержки ее работоспособности. Надо помнить, что резервирование функций удорожает всю систему. Стремление многократно и надежно резервировать функции системы вступает в противоречие двум важнейшим инженерным принципам: во-первых, надежность системы обратно пропорцио-

нальна количеству составляющих ее компонент, во-вторых, надежность системы не может быть выше, чем у наименее надежного компонента. В реальности СУиК ЯМ не требуют столь жестких нормативов, как АС ФЗ. Отраслевой стандарт устанавливает максимальное время восстановления работоспособности СУиК ЯМ – не более 10 часов. Подчеркивается, что этот норматив устанавливается для каждой конкретной подсистемы на стадии разработки компьютеризированной СУиК ЯМ.

Для аварийного восстановления работоспособности системы в случае потери всей информации необходимо восстановить базовое и прикладное программное обеспечение и содержимое баз данных. Этим целям служат хранение дистрибутивов программного обеспечения и резервных копий баз данных. Стандарт выделяет два требования к хранению резервных копий информации: наличие более чем одной копии и хранение резервных копий отдельно от оригинала, желательно в территориально удаленном месте. В работе [19] приводятся основополагающие принципы, нацеленные на сохранение данных:

1) резервные копии данных делаются не в единственном экземпляре, а в нескольких, как минимум по принципу «дед-отец-сын»;

2) выбираются надежные носители информации для выполнения резервных копий;

3) создаются полноценные резервные копии;

4) обеспечивается надежное хранение резервных копий в отдельном помещении – территориально удаленном от первичного носителя информации;

5) обеспечивается регулярный контроль качества резервных копий и пригодность к восстановлению.

Данные принципы обеспечивают восстановление данных ценой некоторых временных затрат. Однако следовать им надо неукоснительно. Так, если резервные копии хранятся в серверном помещении, то с точки зрения восстановления информации их ценность практически нулевая. В случае пожара они погибнут вместе с оригиналом.

Стандарт определяет максимальное значение среднего времени наработки на сбой СУиК ЯМ в 250 часов. Определяется, что используемая вычислительная техника должна быть отнесена к пятому классу и соответствовать требованиям надежности по ГОСТ

27201. Помещения, в которых размещаются элементы автоматизированной системы, должны соответствовать требованиям пожарной и общепромышленной безопасности по ГОСТ 12.4.009.

Нельзя сбрасывать со счетов и человеческий фактор. Низкий уровень подготовки персонала и безответственное отношение к своим обязанностям часто приводит к отсутствию стратегии резервирования и восстановления данных или их разработке на формальном уровне, с нарушением принципов и правил. По оценкам специалистов до 75% всех резервных копий являются непригодными к восстановлению. Эта оценка сделана в отношении западных компаний.

Для учета человеческого фактора стандарт отрасли выделяет в отдельный параграф вопросы организационного обеспечения. Стандарт требует разработки на каждом предприятии комплекта документов, устанавливающих организационную структуру, права и обязанности персонала, эксплуатирующего СУиК ЯМ. Документы должны определять:

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

• 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.

Каждому предприятию предлагается разработать требования к уровню подготовки, квалификации и количеству специалистов, требующихся для обслуживания СУиК ЯМ. Требуется разработать программы обучения и переподготовки специалистов.

В мире существуют различные системы критериев оценки надежности информационных систем. В качестве примера можно рекомендовать критерии, разработанные некоммерческими организациями Американского института сертифицирования государственных служб бухгалтерского учета AICPA и Канадского института присяжных бухгалтеров CICA. Обзор этих критериев приведен в работе [20]. Однако рассмотрение этих критериев выходит за рамки рассматриваемых в данном пособии проблем.

СПИСОК ЛИТЕРАТУРЫ

1. Стандарт отрасли. Оснащение программно-аппаратных систем учета и контроля ядерных материалов. Общие требования. ОСТ 95 10537-97.

2. Зегжда Д.П., Ивашко А.М. Основы безопасности информационных систем. М.: Горячая линия – Телеком, 2000.

3. Правила физической защиты ядерных материалов, ядерных установок и пунктов хранения ядерных материалов. Утверждены Постановлением Правительства Российской Федерации от 19 июля 2007 г. N 456.

4. Требования к системам физической защиты ядерных материалов, ядерных установок и пунктов хранения ядерных материалов. НП-083-07. Федеральная служба по экологическому, технологическому и атомному надзору.

5. Пискарев А.С., Шеин А.В. О состоянии и перспективах использования Общих критериев оценки безопасности информационных технологий в России для оценки применяемых в СУиК программных средств // Материалы 5 международного рабочего семинара «Разработка Федеральной автоматизированной информационной системы учета и контроля ядерных материалов России», г. Новоуральск, Свердловской обл., 26-30 мая 2003 г.

6. Гостехкомиссия России. Руководящий документ. Концепция защиты средств вычислительной техники от несанкционированного доступа к информации. М., 1992.

7. Гостехкомиссия России. Руководящий документ. Средства вычислительной техники. Защита от несанкционированного доступа к информации. Показатели защищенности от несанкционированного доступа к информации. М., 1992.

8. Гостехкомиссия России. Руководящий документ. Автоматизированные системы. Защита от несанкционированного доступа к информации. Классификация автоматизированных систем и требования по защите информации. М., 1992.

9. Гостехкомиссия России. Руководящий документ. Временное положение по организации разработки, изготовления и эксплуатации программных и технических средств защиты информации от несанкционированного доступа в автоматизированных системах и средствах вычислительной техники. М., 1992.

10. Гостехкомиссия России. Руководящий документ. Защита от несанкционированного доступа к информации. Термины и определения. М., 1992.

11. Гостехкомиссия России. Министерство Российской Федерации по атомной энергии. Руководящий документ. Требования по защите от несанкционированного доступа к информации в автоматизированных системах учета и контроля ядерных материалов. М., 1997.

12. Международное исследование в области компьютерной безопасности (обзор) – **www.crime-research.ru/news/2003/07/2403.html**

13. Государственный стандарт Российской Федерации. ГОСТ Р ИСО/МЭК 15408-1-2001. Информационная технология. Методы и средства обеспечения безопасности критерии оценки безопасности информационных технологий. Часть 1. Введение и общая модель.

14. Государственный стандарт Российской Федерации. ГОСТ Р ИСО/МЭК 15408-2-2001. Информационная технология. Часть 2.

15. Государственный стандарт Российской Федерации. ГОСТ Р ИСО/МЭК 15408-2-2001. Информационная технология. Часть 3.

16. Федеральный Закон РФ от 27.12.2002 № 184-ФЗ «О техническом регулировании».

17. Вихорев С. ГОСТ на европейский лад, или Меняем не глядя? // Сети, 2003, №2. М.: Открытые системы. Постоянный адрес статьи **http://www.osp.ru/nets/2003/02/032.htm**

18. Короткин Д. Обеспечение физической безопасности устранит 39% угроз. Аналитическое приложение. – **www.cnews.ru/newcom/index.html?2003/10/15/150071**

19. Воинов Ю. Новоиндийская защита или катастрофоустойчивые решения по защите данных.– **www.softdeco.com/index.php**

20. Решение проблемы доверия к Интернет и информационным технологиям в электронных правительствах и электронном бизнесе. – Центр компетенции по электронному правительству при Американской Торговой Палате в России. № 0045/R 25.02.03.

21. Гостехкомиссия России. Руководящий документ. Руководство по разработке профилей защиты и заданий по безопасности, 2003.

22. Гостехкомиссия России. Руководящий документ. Безопасность информационных технологий. Руководство по регистрации профилей защиты, 2003.