Научная серия

Защита информации

Редактор Е. М. Сухарев

КНИГА 2

ОБЕСПЕЧЕНИЕ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ В ЭКОНОМИЧЕСКОЙ И ТЕЛЕКОММУНИКАЦИОННОЙ СФЕРАХ

Издательство «Радиотехника»
Москва 2003

УДК 519.6
О13
ББК 32.811

Библиотека журнала «Радиотехника»

Серия «Защита информации»

Редактор Е. М. Сухарев

Авторы см. с. 207-211

Книга 2

Обеспечение информационной безопасности в экономической и телекоммуникационной сферах

О13 Обеспечение информационной безопасности в экономической и телекоммуникационной сферах. Коллективная монография. / Под ред. *Е. М. Сухарева*. Кн. 2. – М.: Радиотехника, 2003. — 216 с.: ил. (Сер. Защита информации. Редактор Е. М. Сухарев).

ISBN 5-93-108-053-8

Показано развитие методов и средств защиты информации в кредитно-финансовой сфере России, создание автоматизированной системы формирования защищенной консолидированной финансовой отчетности; приведены результаты исследований при формировании и введении в гражданско-правовой оборот объектов интеллектуальной собственности, рассмотрены новые технические решения при обеспечении информационной безопасности в экономической и телекоммуникационной сферах.

Для инженеров и научных работников; может быть полезна преподавателям и студентам, а также специалистам, занимающимся вопросами защиты информации.

УДК 519.6
ББК32.811

ISBN 5-93-108-053-8

Содержание

II.4. Защита информации как неотъемлемая часть информационной поддержки жизненного цикла сложных высокотехнологичных систем*

Обращение информации различного назначения в системах передачи данных корпоративных объединений разработчиков и изготовителей сложных высокотехнологичных систем является одной из базовых функций информационной поддержки жизненного цикла (ЖЦ) создаваемых систем. При этом важнейшим фактором становится ЗИ (данных) от утечки, искажения, утраты при обработке, хранении и передаче. Защита информации должна предотвращать не только угрозу несанкционированного ознакомления со служебной (конфиденциальной, секретной) информацией, но и угрозу ее несанкционированной модификации, уничтожения, навязывания ложной информации, возможность принятия руководством неадекватных реальной обстановке решений. Недооценка важности ЗИ, в конечном счете, может привести не только к утрате сведений, составляющих коммерческую или государственную тайну, но к выводу сложных высокотехнологичных систем в целом из строя.

Системы информационной поддержки ЖЦ сложных высокотехнологичных систем выполняют свои функции (по тем или иным разрабатываемым методам) посредством сбора, хранения, обработки и представления информации на основе интеграции возможностей вычислительных комплексов, программных средств, средств связи и человека. В связи с этим требования к функционированию информационной поддержки ЖЦ формируются с учетом реализации целей создания и эксплуатации перспективных образцов сложных высокотехнологичных систем, условий использования системы информационной поддержки, выделяемых ресурсов на создание и эксплуатацию этой системы, требований со стороны управляемых объектов, а также требований и условий взаимодействия с другими, внешними по отношению к рассматриваемой, системами.

Требуемые характеристики, отвечающие целям функционирования информационной поддержки ЖЦ сложных высокотехнологичных систем, представлены на рис. 1.

Следует учитывать, что интегральное качество используемой в информационной поддержке ЖЦ сложных систем информации существенным образом зависит от типов решаемых функциональных задач, содержания получаемой в результате решения задач выходной инфор-

* Авторы: В. М. Алдошин, И. Р. Ашурбейли

мации и требований пользователей в конкретных условиях функционирования системы. Эти зависимости должны учитываться при детальной оценке систем и обосновании требований при разработке методов информационной поддержки ЖЦ.

Рис. 1. Характеристики, отвечающие целям функционирования информационной поддержки ЖЦ сложных высокотехнологичных систем

Рассмотрим более подробно приведенные характеристики системы информационной поддержки ЖЦ [1,2,3,4]:

устойчивость системы – способность системы продолжать нормальную работу (согласно функциональному алгоритму осуществлять сбор, хранение, обработку, представление информации) после сбоев и отказов аппаратуры или неверных действий персонала:

своевременность представления требуемой информации (выполнения технологической операции) – свойство системы обеспечивать представление запрашиваемой или выдаваемой выходной информации (выполнения технологической операции по команде или автоматически) в задаваемые сроки, гарантирующие выполнение соответствующей функции согласно целевому назначению системы;

полнота информации – свойство выходной информации отражать состояние всех требуемых объектов управления, слагается из полноты реализации функций системы информационной поддержки ЖЦ, полноты первоначального наполнения баз данных и полноты отражения в базах данных новых объектов;

достоверность информации (данных) – свойство информации быть правильно воспринятой (вероятность отсутствия ошибок); ее мож-

но рассматривать как степень соответствия данных, хранимых в памяти ЭВМ, в базах данных или документах, реальному состоянию отображаемых ими объектов предметной области; определяется достоверностью ранее обработанной информации, безошибочностью и актуальностью необработанной исходной информации, используемой для ее получения, а также точностью обработки и достоверностью передачи информации;

актуальность информации – свойство входной информации, подлежащей последующей функциональной обработке, отражать текущее состояние объектов и процессов прикладной области системы информационной поддержки ЖЦ ВВТ со степенью приближения, достаточной для получения на ее основе достоверной выходной информации;

безошибочность действий персонала – отсутствие случайных ошибок со стороны пользователей и обслуживающего персонала;

отсутствие вирусных воздействий – недопущение воздействия компьютерных вирусов на программы, файлы, каталоги, вычисления, память и работу ЭВМ при копировании с диска на диск либо по вычислительной сети;

безопасность данных – защита данных и программ от несанкционированного доступа (НСД) к ним, осуществляемого с целью раскрытия, изменения или разрушения данных; достигается применением аппаратных, программных и криптографических методов и средств защиты, а также комплексом организационных мероприятий.

Обоснование системотехнических требований к качеству функционирования системы информационной поддержки ЖЦ сложных систем заключается во взаимоувязанной оценке показателей ее устойчивости, своевременности представления, полноты, достоверности и безопасности используемой информации (данных).

При разработке методов информационной поддержки ЖЦ сложных систем и формировании проектов создания систем информационной поддержки необходимо учитывать следующие базовые принципы:

системность – анализ методов и проектов должен быть направлен на оценку степени достижения целей функционирования систем информационной поддержки ЖЦ;

объективность – сравнение методов и проектов должно осуществляться по одному интегральному показателю, зависящему от множества количественных требований, характеристик и условий эксплуатации.

Суть принятия решения по выбору предлагаемых (разработанных) методов (проектов) информационной поддержки ЖЦ сложных систем состоит в том, что предпочтение отдается тому методу (проекту), который при прочих равных условиях способен за счет более эффективных

технических решений или меньшей стоимости работ реализовать более высокое качество информационной поддержки, включающей надежную защиту информации.

Руководствуясь приведенными выше принципами системности и объективности, можно использовать интегральный показатель C, характеризующий степень достижения цели функционирования системы информационной поддержки ЖЦ ВВТ на единицу затрат ресурсов [3]:

$$C = C_{\text{жц}} / S_{\text{м}},$$

где $C_{\text{жц}}$ – интегральный показатель, характеризующий вероятность устойчивой работы и своевременного представления полной, достоверной и защищенной информации в системе информационной поддержки ЖЦ сложных систем; $S_{\text{м}}$ – затраты ресурсов на реализацию метода (проекта) информационной поддержки ЖЦ.

Интегральный показатель определяется выражением

$$C_{\text{жц}} = f(P_{\text{уст}}, P_{\text{св}}, P_{\text{пол}}, P_{\text{дост}}, P_{\text{без}}),$$

где $f(P)$ – интегрирующая функциональная зависимость, характеризующая качество функционирования системы информационной поддержки ЖЦ с учетом ее структуры, условий эксплуатации и предлагаемых проектных решений; $P_{\text{уст}}$ – вероятность устойчивости системы информационной поддержки; $P_{\text{св}}$ – вероятность своевременного представления требуемой информации (выполнения технологической операции); $P_{\text{пол}}$ – вероятность того, что информация в системе полно отражает состояние всех требуемых объектов управления; $P_{\text{дост}}$ – вероятность обеспечения достоверности информации (данных); $P_{\text{без}}$ – вероятность безопасности данных.

Определим вероятность $P_{\text{дост}}$:

$$P_{\text{дост}} = P_{\text{акт}} P_{\text{пер}} P_{\text{вир}} P_{\text{защ}},$$

где $P_{\text{акт}}$ – вероятность сохранения актуальности информации на момент ее использования; $P_{\text{пер}}$ – вероятность обеспечения безошибочности функциональных и технологических действий пользователей и обслуживающего персонала; $P_{\text{вир}}$ – вероятность безопасного функционирования системы в условиях вирусного воздействия; $P_{\text{защ}}$ – вероятность сохранения защищенности системы от НСД.

Значения приведенных вероятностей могут быть заданы в рамках формируемых требований при разработке методов (проектов) информационной поддержки ЖЦ сложных высокотехнологичных систем.

Защита информации в современных условиях, во многом связанных с формированием корпоративных объединений разработчиков и изготовителей наукоемкой продукции, становится одной из наиболее весомых составляющих качества функционирования системы информационной поддержки ЖЦ сложных высокотехнологичных образцов техники.

Литература

1. *Алдошин В.М., Колганов С.К., Фефилатьев В.П.* Корпоративные информационные технологии в управлении интегрированной структурой. – Вопросы оборонной техники. Сер. 3, 2001, № 3.
2. *Ашурбейли И.Р., Рухадзе К.В., Спокойный М.Ю., Фетодов А.Г.* Программа реализации закрытого канала передачи данных с гарантированной доставкой// Труды LVII научной сессии Российского научно-технического общества радиотехники, электроники и связи им. А.С.Попова. – 2000.
3. *Безкоровайный М.М., Костогрызов А.И., Львов В.М.* Инструментально-моделирующий комплекс для оценки качества функционирования информационных систем «КОК». Руководство системного аналитика. – М.: СИНТЕГ. 2000.
4. *Першиков В.И., Савинков В.М.* Толковый словарь по информатике. – М.: Финансы и статистика, 1991.

II.5. Основные направления обеспечения информационной безопасности на высокотехнологичных предприятиях*

Высокотехнологичные предприятия, разрабатывающие и выпускающие наукоемкую продукцию, характеризуются большими объемами информационных потоков, которые во многом носят конфиденциальный характер. Развитие средств, методов и форм автоматизации хранения и обработки информации, массовое применение персональных компьютеров с объединением их в локальные вычислительные сети делают информацию гораздо более уязвимой. Циркулирующая в автоматизированных системах (АС) информация может быть незаконно изменена, похищена или уничтожена. Поэтому основной проблемой создания и эксплуатации информационных АС является обеспечение безопасности хранимых и передаваемых данных, требующее разработки комплекса мер обеспечения безопасности, направленных на предотвращение несанкционированного получения информации, физического уничтожения или модификации защищаемой информации.

Основные понятия, требования, методы оценки системы информационной безопасности, которые могут быть использованы высокотехнологичными предприятиями, разрабатывающими и выпускающими наукоемкую продукцию, отражены в ряде основополагающих документов:

«Оранжевой книге» Национального центра защиты компьютеров США (TCSEC);

Гармонизированные критерии Европейских стран (ITSEC);

Рекомендации X.800;

Концепция защиты от несанкционированного доступа Гостехкомиссии при Президенте Российской Федерации.

«Оранжевая книга» Национального центра защиты компьютеров США *(TCSEC)* – документ, который был впервые опубликован в августе 1983 г. в Министерстве обороны США. В нем дается пояснение понятия *«безопасная система»,* которая «управляет посредством соответствующих средств доступом к информации так, что только авторизованные лица или процессы, действующие от их имени, получают право читать, писать, создавать и удалять информацию».

В «Оранжевой книге» степень доверия, или надежность проектируемой или используемой системы защиты и ее компонентов оце-

* Авторы: И. Р. Ашурбейли, В. И. Соловьев

нивается по двум основным критериям: *концепции безопасности* и *гарантированности.*

Концепция безопасности разрабатываемой системы – «это набор законов, правил и норм поведения, определяющих, как организация обрабатывает, защищает и распространяет информацию. В частности, правила определяют, в каких случаях пользователь имеет право оперировать с определенными наборами данных. Чем надежнее система, тем строже и многообразнее должна быть концепция безопасности. В зависимости от сформулированной концепции можно выбирать конкретные механизмы, обеспечивающие безопасность системы. Концепция безопасности – это активный компонент защиты, включающий в себя анализ возможных угроз и выбор мер противодействия».

Гарантированность – «мера доверия, которая может быть оказана архитектуре и реализации системы. Гарантированность может проистекать как из тестирования, так и из проверки общего замысла и исполнения системы в целом и ее компонентов. Гарантированность показывает, насколько корректны механизмы, отвечающие за проведение в жизнь выбранной концепции безопасности. В «Оранжевой книге» рассматриваются два вида гарантированности: *операционная* и *технологическая.* Операционная гарантированность относится к архитектурным и реализационным аспектам системы, в то время как технологическая – к методам построения и сопровождения.

Операционная гарантированность – это способ убедиться в том, что архитектура системы и ее реализация действительно проводят в жизнь избранную концепцию безопасности и включают в себя проверку основных элементов системы. При этом происходит следующее:

архитектура системы способствует реализации мер безопасности или прямо поддерживать их. Примеры подобных архитектурных решений в рамках аппаратуры и операционной системы – разделение команд по уровням привилегированности, защита различных процессов от взаимного влияния за счет выделения каждому своего виртуального пространства, особая защита ядра операционной системы. Архитектура системы должна обеспечивать возможность установки дополнительных защитных продуктов, повышающих надежность как отдельных компонентов, так и всей системы;

целостность системы означает, что аппаратные и программные компоненты надежной вычислительной базы работают должным образом и имеется аппаратное и программное обеспечение для периодической проверки целостности;

анализ тайных каналов передачи информации позволяет обеспечить конфиденциальность информации. Обычно тайные каналы используются не столько для передачи информации от одного злоумышленни-

ка к другому, сколько для получения злоумышленником сведений от внедренного в систему «троянского коня»;

надежное администрирование определяет роли системного администратора, системного оператора и администратора безопасности;

надежное восстановление после сбоев включает два вида деятельности: подготовку к сбою (отказу) и собственно восстановление, и обеспечивает гарантированность, при которой должна быть сохранена целостность информации.

Технологическая гарантированность охватывает весь жизненный цикл системы от проектирования, реализации, тестирования, внедрения до сопровождения. Все перечисленные действия должны выполняться в соответствии с требованиями стандартов, чтобы обезопасить систему от утечки информации и нелегальных «закладок».

Критерии, изложенные в «Оранжевой книге», ранжируют информационные системы ЗИ по степени безопасности на четыре уровня, два из которых подразделяются на классы. Чтобы система в результате процедуры сертификации могла быть отнесена к некоторому классу, ее концепция безопасности и гарантированность должны удовлетворять разработанной системе требований, соответствующей этому классу.

Следуя по пути интеграции, европейские страны приняли согласованные (гармонизированные) критерии оценки безопасности информационных технологий (Information Technology Security Evaluation Criteria, ITSEC), опубликованные в июне 1991 г. от имени соответствующих органов четырех стран – Франции, Германии, Нидерландов и Великобритании.

Принципиальной особенностью европейских критериев является отсутствие априорных требований к условиям, в которых должна работать информационная система. Каждая организация, запрашивающая сертификационные услуги, формулирует необходимые цели оценки и описывает условия, в которых должна работать система, возможные угрозы ее безопасности и предоставляемые ею защитные функции. Задача органа сертификации – оценить, насколько полно достигаются поставленные цели разработанными функциями, а также насколько корректны и эффективны архитектура и реализация механизмов безопасности в описанных разработчиком условиях.

Европейские критерии рассматривают следующие основные понятия, составляющие базу информационной безопасности:

конфиденциальность – защиту от несанкционированного получения информации;

целостность – защиту от несанкционированного изменения информации;

доступность – защиту от несанкционированного удержания информации и ресурсов.

Критерии рекомендуют выделить в спецификациях реализуемых функций обеспечения безопасности следующие процедуры: идентификацию и аутентификацию, управление доступом, подотчетность, аудит, повторное использование объектов, точность информации, надежность обслуживания, обмен данными.

Европейские критерии в качестве приложения содержат описание десяти примерных классов функциональности, типичных для правительственных и коммерческих систем, пять из которых соответствуют классам безопасности «Оранжевой книги».

В критериях определены три мощности механизмов защиты: *базовая, средняя* и *высокая.* Согласно критериям, мощность можно считать *базовой*, если механизм способен противостоять отдельным случайным атакам; *средней* – если механизм способен противостоять злоумышленникам с ограниченными ресурсами и возможностями; *высокой* – если механизм защиты может быть взломан злоумышленником с высокой квалификацией.

В 1992 г. Гостехкомиссия при Президенте Российской Федерации опубликовала пять руководящих документов, посвященных проблеме защиты от несанкционированного доступа к информации. Основой руководящих документов является «Концепция защиты средств вычислительной техники и автоматизированных систем от несанкционированного доступа к информации». Концепция «излагает систему взглядов, основных принципов, которые закладываются в основу проблемы защиты информации от НСД, являющейся частью общей проблемы безопасности информации».

Существуют различные способы покушения на информационную безопасность: радиотехнические, акустические, программные и т.п. Среди них НСД выделяется как доступ к информации, нарушающий установленные правила разграничения доступа, с использованием штатных средств, предоставляемых средствами вычислительной техники (СВТ) или АС. Под *штатными средствами* понимается совокупность программного, микропрограммного и технического обеспечения СВТ или АС.

В Концепции формулируются следующие основные принципы защиты АС от НСД к информации:

обеспечение ЗИ комплексом программно-технических средств и поддерживающих их организационных мер;

обеспечение защиты на всех технологических этапах обработки информации и во всех режимах функционирования, в том числе при проведении ремонтных и регламентных работ;

программно-технические средства защиты не должны существенно ухудшать основные функциональные характеристики АС (надежность, быстродействие, возможность изменения конфигурации АС);

оценка эффективности средств защиты, осуществляемая по методике, учитывающей всю совокупность технических характеристик оцениваемого объекта, включая технические решения и практическую реализацию средств защиты;

контроль эффективности средств защиты от НСД.

Функции системы разграничения доступа и обеспечивающих средств, предлагаемые в Концепции, по сути близки к аналогичным положениям «Оранжевой книги».

В предлагаемой Гостехкомиссией при Президенте Российской Федерации классификации автоматизированных систем по уровню защищенности от несанкционированного доступа к информации установлено девять классов защищенности АС от НСД к информации. Каждый класс характеризуется определенной минимальной совокупностью требований по ЗИ, а также подразделяется на три группы, учитывающие особенности обработки информации в АС. В пределах каждой группы соблюдается иерархия требований по защите в зависимости от ценности (конфиденциальности) информации.

Основополагающим документом в области защиты распределенных систем стали *Рекомендации X.800*. В этом документе перечислены основные сервисы (функции) безопасности, характерные для распределенных систем, и роли, которые они могут играть; указан перечень основных механизмов, с помощью которых можно реализовать эти сервисы.

«Оранжевая книга» Министерства обороны США и Руководящие документы Гостехкомиссии при Президенте Российской Федерации создавались в расчете на централизованные конфигурации СВТ, основу которых составляют большие машины. Широкое внедрение персональных компьютеров, средств коммуникаций, распределенная организация современных информационных систем, появление новых типов машинных носителей информации требует внесения существенных изменений и дополнений как в политику безопасности, так и в способы проведения их в жизнь. Появились новые угрозы, для противодействия которым нужны новые функции и механизмы защиты.

В связи с быстрым устареванием существующих стандартов одним из основных направлений обеспечения информационной безопасности на высокотехнологичных предприятиях следует считать разработку

профиля ЗИ, представляющего собой совокупность нескольких (или подмножество одного) базовых стандартов с четко определенными и гармонизированными подмножествами обязательных и факультативных возможностей, предназначенная для реализации функций ЗИ. Профиль ЗИ должен формироваться, исходя из функциональных характеристик объекта стандартизации, в нем должны быть выделены и установлены допустимые возможности и значения параметров каждого базового стандарта и/или нормативного документа, входящего в профиль.

Существуют две группы профилей: регламентирующие архитектуру и структуру системы ЗИ; регламентирующие процессы проектирования, разработки, применения, сопровождения и развития системы ЗИ.

Профиль конкретной системы защиты не является статичным, он может развиваться и конкретизироваться в процессе проектирования или эксплуатации информационной системы, с последующим оформлением в составе документации проекта системы или рабочей документации.

В профиль конкретной системы защиты могут включаться спецификации компонентов, разработанных в составе данного проекта или действующей системы, спецификации использованных готовых программных и аппаратных средств, если эти средства не специфицированы соответствующими стандартами. После завершения проектирования и испытаний системы, в ходе которых проверяется ее соответствие профилю, профиль применяется как основной инструмент сопровождения системы при эксплуатации, модернизации и развитии.

Формирование и применение профилей конкретных систем ЗИ может выполняться на основе использования международных и национальных стандартов, ведомственных нормативных документов, а также стандартов де-факто при условии доступности соответствующих им спецификаций.

Одним из важнейших направлений обеспечения информационной безопасности на высокотехнологичных предприятиях в настоящее время является создание профиля ЗИ, передаваемой по каналам связи, которые можно разделить на внутренние (локальные сети предприятия) и внешние (информационное взаимодействие предприятий). Эффективное использование современных информационных технологий требует объединения компьютеров в локальные вычислительные сети, создания баз данных по предметным областям. Такое объединение создает дополнительные каналы утечки информации, что вызывает принятие адекватных мер по ЗИ. Совместная работа предприятий интегрированной структуры требует организации информационного взаимодействия.

Из существующих сегодня способов передачи информации наиболее предпочтительными являются использование выделенных волокон-

но-оптических линий связи и телефонных каналов с использованием модемов и применением метода закрытия информации, заключающегося в установке устройства закрытия информации на уровне стыка между компьютером и коммуникационным оборудованием с установкой на компьютер телекоммуникационного программного обеспечения. Использование программных средств закрытия канала передачи данных с гарантированной доставкой и средств криптозащиты позволит обеспечить передачу конфиденциальной информации по открытым каналам связи.

Достоверность передаваемой по каналам связи информации должна подтверждаться электронной цифровой подписью, внедрение которой на высокотехнологичных предприятиях является в настоящее время насущной задачей.

Создание электронных архивов конструкторско-технологической документации, баз данных и знаний, обмен документацией в электронном виде на машинных носителях информации требует сертификации качества машинных носителей информации.

Профиль ЗИ высокотехнологичного предприятия должен включать следующие основные направления работ по обеспечению информационной безопасности:

определение особенностей хранимой и передаваемой информации, выявление видов угроз и возможных каналов утечки информации;

выбор концепции и принципов построения системы защиты, также разработку функциональной структуры системы защиты хранимой, обрабатываемой и передаваемой информации;

разработку критериев оценки операционной и технологической гарантированности защиты информации;

разработку или выбор из предлагаемого программного обеспечения системы защиты (программные средства, реализующие выбранные механизмы защиты, должны быть подвергнуты комплексному тестированию);

определение системы физических мер охраны СВТ (устройств и носителей информации), предусматривающие постоянную охрану территории и здания, где размещаются автоматизированные информационные системы, с помощью как технических средств охраны, так и специального персонала, а также строгий пропускной режим, специальное оборудование помещений автоматизированных информационных систем, соблюдение противопожарных требований;

сертификацию используемых средств вычислительной и организационной техники и машинных носителей информации;

установку программно-технических средств защиты от НСД;

проведение организационных мероприятий по РВ.

При этом проведение организационных мероприятий по ЗИ должно включать:

создание службы (назначение администратора) администрирования системы ЗИ, ответственной за ведение, нормальное функционирование и контроль работы средств ЗИ от НСД с предоставлением терминала и необходимых средств оперативного контроля и воздействия на безопасность АС;

наличие средств восстановления средств ЗИ от НСД, предусматривающих ведение двух копий программных средств ЗИ от НСД и их периодическое обновление и контроль работоспособности;

использование сертифицированных средств защиты;

периодическое тестирование всех функций средств ЗИ от НСД с помощью специальных программных средств;

составление документации, как необходимое условие гарантированной надежности системы и одновременно инструмент проведения выбранной концепции безопасности.

В комплект документации надежной системы должны входить: руководство пользователя по средствам безопасности, руководство администратора по средствам безопасности, тестовая документация, описание архитектуры.

В основу создания базовой системы ЗИ в АС в целом и для информационной базы, в частности, могут быть положены следующие основные принципы:

оптимального сочетания программных, аппаратных средств и организационных мер защиты;

разделения и минимизации полномочий по доступу к обрабатываемой информации и процедурам обработки;

полноты контроля и регистрации попыток несанкционированного доступа;

обеспечения надежности системы защиты.

Систему безопасности можно разделить на две части: внутреннюю и внешнюю. Во *внутренней* части осуществляется в основном контроль доступа пользователей в сеть и базу данных. Помимо этого шифруются и идентифицируются данные во время их передачи и хранения.

Безопасность *внешней* части системы может быть достигнута применением криптографических методов в сочетании с использованием соответствующих аппаратных средств. Аппаратные средства защиты реализуют функции разграничения доступа, криптографии, контроля целостности программ и их защиты от копирования во внутренней части, хорошо охраняемой административно.

Перечисленные требования составляют минимум, которому необходимо следовать, чтобы обеспечить конфиденциальность защищаемой информации на высокотехнологичном предприятии.

Литература

1. Гостехкомиссия России. Руководящий документ. Автоматизированные системы. Защита от несанкционированного доступа к информации и требования по защите информации. – М.: Воениздат, 1992.
2. Гостехкомиссия России. Руководящий докумснт. Защита от несанкционированного доступа к информации. Термины и определения. –М.: Воениздат, 1992.
3. Гостехкомиссия России. Руководящий документ. Концепция защиты средств вычислительной техники средств вычислительной техники и автоматизированных систем от несанкционированного доступа к информации. – М.: Воениздат, 1992.
4. Гостехкомиссия России. Руководящий документ. Средства вычислительной техники. Защита от несанкционированного доступа к информации. Показатели защищенности от несанкционированного доступа к информации. – М.: Воениздат, 1992.
5. *Смирнова Г.Н., Сорокин А.А., Тельнов Ю.Ф.* Проектирование экономи-ческих информационных систем. – М.: Финансы и статистика, 2001.
6. Security Architecture for Open Systems Interconnection for CCITT Aplications. Recommendation X.800 – CCITT. – Geneva, 1991.