

Министерство образования Республики Беларусь  
БЕЛОРУССКИЙ НАЦИОНАЛЬНЫЙ ТЕХНИЧЕСКИЙ  
УНИВЕРСИТЕТ

---

Кафедра «Информационно-измерительная техника и технологии»

В.А. Артамонов

ПРОЕКТИРОВАНИЕ СИСТЕМ ЗАЩИТЫ  
КОМПЬЮТЕРНОЙ ИНФОРМАЦИИ

Методическое пособие  
по курсовому проектированию

Минск  
БНТУ  
2011

УДК 004.056.5:378.147.091.313 (075.8)

ББК 32.81я7

А 86

**Р е ц е н з е н т ы:**

*И.Н. Цырельчук*, канд. техн. наук, доц., заведующий кафедрой  
«Радиоэлектронные средства» БГУИР;

*К.Л. Тявловский*, канд. физ.-мат. наук, доц. кафедры  
«Информационно-измерительная техника и технологии» БНТУ

**Артамонов, В.А.**

А 86 Проектирование систем защиты компьютерной информации: методическое пособие по курсовому проектированию / В.А. Артамонов. – Минск: БНТУ, 2011. – 65 с.

ISBN 978-985-525-432-5.

Пособие содержит краткие сведения о требованиях к составу и объему курсового проекта, правилах выполнения курсового проекта по дисциплине «Проектирование систем защиты компьютерной информации». В нем изложены методические основы, нормативные требования и правила оценки достигнутого уровня защищенности, применяемые при защите информации от несанкционированного раскрытия, модификации или потери возможности ее использования.

Настоящее методическое пособие применимо к выполнению курсовых проектов в области аппаратных, аппаратно-программных и программных средств безопасности продуктов и систем информационно-коммуникационных технологий (ИКТ). Если отдельные аспекты методики проектирования и/или оценки применимы только для определенных способов реализации продуктов или систем ИКТ, а также объектов информатизации, то это отмечается при формулировании задания по курсовому (дипломному) проектированию.

Пособие может использоваться студентами специальности 1-38 02 03 «Техническое обеспечение безопасности» специализации 1-38 02 03-02 «Аппаратно-программные средства защиты компьютерной информации», а также студентами других специальностей при курсовом и дипломном проектировании в случае наличия в составе их работ разделов, связанных с информационной безопасностью.

УДК 004.056.5:378.147.091.313 (075.8)  
ББК 32.81я7

ISBN 978-985-525-432-5

© Артамонов В.А., 2011

© БНТУ, 2011

## ОГЛАВЛЕНИЕ

ВВЕДЕНИЕ.....	4
1. ТРЕБОВАНИЯ К СОСТАВУ И ОБЪЕМУ КУРСОВОГО ПРОЕКТА.....	5
1.1. Примерная тематика проектов.....	12
1.2. Разработка технического задания.....	13
2. ВЫПОЛНЕНИЕ СХЕМ КУРСОВОГО ПРОЕКТА.....	16
2.1. Структурная схема устройства.....	18
2.2. Функциональная схема устройства.....	18
2.3. Схема электрическая принципиальная.....	19
2.4. Схемы монтажные, подключения, расположения.....	21
2.5. Выполнение блок-схемы алгоритма программы.....	21
2.6. Выполнение функциональных схем проекта верхнего или нижнего уровня.....	31
2.7. Разработка профиля защиты.....	34
2.7.1. Общие положения.....	34
2.7.2. Содержание профиля защиты.....	34
2.8. Разработка задания по безопасности.....	41
2.8.1. Общие положения.....	41
2.8.2. Содержание задания по безопасности.....	41
3. МЕТОДОЛОГИЯ ОЦЕНКИ УРОВНЯ ЗАЩИЩЕННОСТИ ПРОДУКТОВ И СИСТЕМ ИНФОРМАЦИОННЫХ ТЕХНОЛОГИЙ.....	51
3.1. Общая методология оценки.....	51
3.2. Процесс оценки сервисов и механизмов информационной безопасности.....	53
3.2.1. Особенности выполнения количественных оценок.....	53
3.2.2. Анализ стойкости функций безопасности как пример выполнения количественных оценок.....	54
3.2.3. Пример анализа стойкости функции безопасности.....	59
4. ВЫПОЛНЕНИЕ ПРОЕКТА В ЭЛЕКТРОННОЙ ФОРМЕ....	61
НОРМАТИВНЫЕ ДОКУМЕНТЫ.....	62

## ВВЕДЕНИЕ

Курсовой проект (КП) представляет собой самостоятельную работу студента, которая выполняется для развития навыков инженерной деятельности. Основная задача курсового проекта – привить студенту практические навыки разработки и применения средств и систем обеспечения информационной безопасности (ИБ) продуктов и систем информационно-коммуникативных технологий (ИКТ), а также объектов информатизации, научить студентов обосновывать самостоятельно принимаемое проектное решение.

Объектом проектирования является продукт или система ИКТ с выбранными по заранее разработанным требованиям (профиль защиты или задание по обеспечению информационной безопасности) средствами информационной безопасности, сервис безопасности, самостоятельно реализующий ту или иную группу механизмов обеспечения и управления информационной безопасностью, экспертная либо инструментальная система для оценки безопасности систем ИКТ, информационно-измерительная, контролирующая либо управляющая система (устройство), включающая электронные блоки, а также функциональный микропроцессорный блок объектовой подсистемы с соответствующим программным обеспечением, имеющий самостоятельное функциональное значение для контроля (предотвращения) утечки информации по техническим каналам. Задание формируется так, чтобы студент получил навыки инженерной деятельности, связанной с проектированием продуктов и систем ИКТ (объектов информатизации) в защищенном исполнении, с учетом и анализом угроз информационной безопасности и проведением оценки достигнутого в результате уровня защищенности.

## 1. ТРЕБОВАНИЯ К СОСТАВУ И ОБЪЕМУ КУРСОВОГО ПРОЕКТА

При курсовом проектировании выполняются следующие виды работ:

1. Анализ задания и обоснование выбора варианта реализации продукта или системы ИКТ в защищенном исполнении, сервиса ИБ, реализующего те или иные механизмы защиты или системы для оценки или управления ИБ систем ИКТ (объектов информатизации).

2. Разработка задания по обеспечению ИБ или профиля защиты. Разработка (выбор) и обоснование алгоритмов (механизмов) реализации защитных функций аппаратно-программным или программным комплексом (сервисом) ИБ *(для КП, объектом проектирования которых являются отдельно взятые сервисы обеспечения ИБ продуктов или систем ИКТ)*. Разработка проекта высокого уровня (в отдельных случаях требуется дополнительно разработка проекта низкого уровня) объекта оценки (ОО). Выбор и составление функциональных спецификаций сервисов безопасности ОО. Разработка структурных и/или функциональных схем аппаратно-программного комплекса, схемных и конструктивных решений, алгоритмов поддерживающего и специального программного обеспечения и исходных текстов программ *(для КП, объектом проектирования которых являются отдельно взятые сервисы обеспечения ИБ продуктов или систем ИКТ)*.

3. Оценка достигнутого уровня защищенности ОО. Технические характеристики аппаратно-программного или программного комплекса обеспечения ИБ и спецификации механизмов защиты продуктов и систем ИКТ, обеспечиваемые данным сервисом *(для КП, объектом проектирования которых являются отдельно взятые сервисы обеспечения ИБ продуктов или систем ИКТ)*.

Тема курсового проекта назначается преподавателем (в отдельных случаях тема КП, по согласованию с руководителем, может быть сформулирована студентом как составная часть НИРС). Тема проекта – это защищенный продукт или система ИКТ, аппаратно-программный комплекс, реализующий те или иные механизмы безопасности, система оценки защищенности или управления ИБ объекта информатизации или другие средства или системы обеспечения ИБ, которые требуется разработать в ходе КП, например:

1. «Защищенная база данных на основе СУБД XYZR».
2. «Защищенная система организации тендерных торгов».

3. «Межсетевой экран экспертного класса».
4. «Система оценки рисков нарушения информационной безопасности объекта информатизации».
5. «Модуль шифрования на основе алгоритма XXX».
6. «Аппаратно-программный комплекс средств защиты информации от несанкционированного доступа».
7. «Аппаратно-программный комплекс создания и распределения ключей открытых ключей по технологии РКІ».
8. «Аппаратно-программный комплекс для измерения (обнаружения) утечки информации по техническим каналам».

Пояснительная записка должна быть сброшюрована, иметь обложку и титульный лист, оформленные в соответствии со стандартом предприятия СТП БНТУ 3.01–2003 «Курсовое проектирование».

Все части пояснительной записки излагаются только на одном языке – русском или белорусском.

Пояснительная записка печатается с использованием ПЭВМ на одной стороне листа белой писчей бумаги. Печать производится шрифтом Times New Roman размером 14 пунктов (заглавия – жирным шрифтом). Для листингов – Courier New размером не менее 10 пунктов. Листы пояснительной записки должны иметь сквозную нумерацию. Формат листа пояснительной записки А4 (210×297 мм). Шрифты разной гарнитуры, выделение текста с помощью рамок, разрядки, подчеркивания рассматриваются как огрехи оформления. Поля: правое – 10 мм, левое – 30 мм, верхнее и нижнее – по 20 мм. Межстрочный интервал следует выбирать из расчета размещения  $40 \pm 2$  строки на листе текста. Абзацы в тексте начинают отступом, равным 1 см. Оформление пояснительной записки должно удовлетворять требованиям к оформлению «Отчета о научно-исследовательской работе» (ГОСТ 7.32–2001).

Пояснительная записка должна содержать перечисленные в табл. 1 разделы. Разделы в пояснительной записке двух типов: нумерованные («Содержание», «Введение», «Заключение» и т.п.) и нумерованные («1. Обзор литературы», «2. Разработка задания по обеспечению информационной безопасности (профиля защиты, сервисов безопасности и т.д.)». Нумерованные разделы обязательны, а их названия не изменяются. Нумерованные разделы имеют названия, обусловленные темой конкретного курсового проекта, например, не «3. Модульная архитектура», а «3. Периферийный модуль сети уда-

ленного филиала предприятия». Состав и наименования нумерованных разделов согласуются с руководителем проекта.

Таблица 1.1

Разделы пояснительной записки

Раздел	Рекомендуемый объем, содержание раздела
Задание по курсовому проекту	<p>Тема задания, например, «Корпоративный модуль подключения удаленных пользователей»</p> <p>Исходные данные для проектирования – это уточняющие требования, конкретизирующие область возможных технических решений. Например:</p> <ul style="list-style-type: none"> <li>– маршрутизатор Cisco IOS Router с поддержкой ВЧС (rIOS-1);</li> <li>– аппаратный клиент ВЧС Cisco VPN 3002;</li> <li>– межсетевой экран Cisco Secure PIX. (rPIX-1);</li> <li>– программный клиент ВЧС Cisco VPN 3000.</li> </ul> <p>Задание по курсовому проекту оформляется на двух сторонах одного листа</p>
Техническое задание	Разрабатывается студентом на первой стадии курсового проектирования и утверждается руководителем проекта
Содержание	1 лист
Введение	1–2 листа. Актуальность темы задания, характеристика области применения
1. Обзор литературы	<p>7–8 листов. Назначение и область применения разрабатываемой системы, продукта ИКТ или сервиса ИБ.</p> <p>Анализ предметной области разработки, существующих технических решений и выбор оптимального решения, отвечающего требованиям задания.</p> <p>Приводимые по тексту сведения и решения должны сопровождаться ссылками на источник</p>
2. Разработка профиля защиты или задания по безопасности	<p>10–15 листов. Профиль защиты (ПЗ) представляет собой типовой набор требований, которым должны удовлетворять продукты и/или системы ИКТ определенного класса (например, операционные системы на компьютерах в органах государственного управления). Базовый профиль защиты должен включать требования к основным (обязательным в любом случае) возможностям применения продукта или системы ИКТ. Производные профили получают из базового путем добавления необходимых пакетов расширения. Задание по безопасности (ЗБ) содержит совокупность требований к конкретной разработке, выполнение которых обеспечивает достижение поставленных целей</p>

Раздел	Рекомендуемый объем, содержание раздела
3. Проект верхнего и нижнего уровня	<p>10–15 листов. Проект верхнего уровня описывает структуру функций безопасности ОО в терминах <b>подсистем</b>. Проект должен идентифицировать все необходимые базовые аппаратные, аппаратно-программные и/или программные средства с представлением функций, обеспечиваемых поддержкой реализуемых этими средствами механизмов защиты, а также все интерфейсы подсистем, выделяя те из них, которые предполагаются видимыми извне. Каждый интерфейс снабжается описанием назначения и методов использования (то же касается и функциональных спецификаций – это означает демонстрацию соответствия функциональным требованиям и позволяет организовать тестирование). Следует выделить подсистемы, осуществляющие политику безопасности. В конечном итоге, проект верхнего уровня должен содержать обоснование того, что выбранные механизмы достаточны для реализации функций безопасности.</p> <p>Проект нижнего уровня (<i>разрабатывается в случае отдельных требований технического задания</i>) предполагает детализацию до уровня <b>модуля</b>. Специфицируются все интерфейсы модулей, реализующих функции безопасности. Обязательным условием является выделение модулей, реализующих политику безопасности, а также предоставление осуществляющих эту политику функций. Взаимосвязи между модулями следует определять в терминах имеющихся функциональных возможностей безопасности и зависимостях от других модулей. Проект нижнего уровня должен содержать описание назначения и методов использования всех интерфейсов модулей, а при необходимости – возможность создания детального отчета о результатах, нештатных ситуациях и отправки уведомления об ошибках</p>



Раздел	Рекомендуемый объем, содержание раздела
<p>4. Схемотехническая часть (для КП, объектом проектирования которых являются отдельно взятые сервисы обеспечения ИБ, выполненные в виде аппаратно-программных комплексов)</p>	<p>4–8 листов. Описание электронной схемы и ее функционирования. Для всех компонентов схемы должно быть приведено их буквенно-цифровое обозначение, наименование, дано пояснение их функционального назначения в схеме.</p> <p>Описание электронных компонентов, использованных при разработке электрической схемы, в том числе компонентов, определенных заданием.</p> <p>Рекомендуемое содержание: обоснование выбора основных активных электронных компонентов устройства, анализ архитектуры и функциональной схемы, расположение выводов компонента, назначение выводов, рабочие параметры, типовые схемы включения (относящиеся к примененному схемному решению), временные диаграммы работы.</p> <p>Простые компоненты (резисторы, конденсаторы), не являющиеся уникальными либо прецизионными, описываются одним-двумя предложениями, обычно включающими такие параметры, как рассеиваемая мощность, напряжение пробоя, полоса рабочих частот, ТКС, ТКЕ.</p> <p>Не рекомендуется приводить подробные описания микропроцессоров, их систем команд, общеизвестных интерфейсов обмена данными, правил монтажа и т.п. При необходимости такой информации достаточно ограничиться краткой характеристикой со ссылкой на литературу.</p> <p>Рекомендуется пояснять работу схемы временными диаграммами состояний ее узлов.</p> <p>Приводится расчет параметров функционального узла (быстродействие, оценка потребляемой мощности).</p> <p>Выполняется анализ достоинств и недостатков (ограничений области применения) устройства</p>
<p>5. Программная часть (для КП, объектом проектирования которых являются отдельно взятые сервисы обеспе-</p>	<p>2–4 листа. Описание разработанных алгоритмов и программ.</p> <p>Для всех блоков разработанных алгоритмов приводится расширенный комментарий с указанием номера блока в алгоритме.</p> <p>Рекомендуется указывать программные средства (среду), использованную при разработке, включая их версии и названия фирм-разработчиков.</p> <p><b>ВНИМАНИЕ!</b> Алгоритмы функционирования устройства</p>

чения ИБ)	представляются в качестве графического материала в приложении. Листинги программ приводятся в приложении
-----------	--

Окончание табл. 1.1

Раздел	Рекомендуемый объем, содержание раздела
Заключение	1 лист. Содержит перечень разработанных документов (с указанием их обозначений), оценку реализованности технических параметров проекта в соответствии с параметрами технического задания, перспективы ее применения
Список использованных источников	<p>1–2 листа. Перечень использованных источников оформляется в соответствии с ГОСТ 7.1–2003 «Библиографическая запись. Библиографическое описание» и состоит из элементов:</p> <p>1) источник – это книга, журнал и т.п.;</p> <p>2) ссылки на сайты Интернета и имена файлов допустимо использовать только для известных мировых производителей электронных компонентов и только как дополнение к названию документа.</p> <p>Например:</p> <p>MSC1210. Precision Analog-to-Digital Converter (ADC) with 8051 Microcontroller and Flash Memory. – Texas Instruments Incorporated. March 2002 – Revised April 2004. Сайт <a href="http://www.ti.com">www.ti.com</a>, файл <a href="#">sbas203b.pdf</a>.</p> <p>Примеры неверных ссылок:</p> <p><a href="http://www.gaw.ru">www.gaw.ru</a>,  <a href="http://www.microchip.com">www.microchip.com</a>,  <a href="file://localhost/H:/iitt/employees_sidorov.htm">file://localhost/H:/iitt/employees_sidorov.htm</a></p>

Приложения (табл. 1.2) включают функциональную и принципиальную электрические схемы устройства с перечнем элементов, алгоритмы функционирования устройства и листинги разработанных программ.

Таблица 1.2

## Приложения

Раздел	Рекомендуемый объем, содержание
Функциональная, принципиальная электрические схемы	<p>Минимальный формат для принципиальной схемы – А3. Руководствоваться ГОСТ 2.702–75 ЕСКД «Правила выполнения электрических схем», ГОСТ 2.709–81 ЕСКД «Правила выполнения электрических схем цифровой вычислительной техники», ГОСТ 2.710–81 ЕСКД «Обозначения буквенно-цифровые в электрических схемах».</p> <p>Условные графические обозначения в электрических схемах см. в ГОСТ 2.721–74, ГОСТ 2.728–74, ГОСТ 2.730–73, ГОСТ 2.743–91, ГОСТ 2.755–87, ГОСТ 2.759–82, ГОСТ 2.764–86.</p> <p>Для всех входных и выходных цепей должны использоваться разъемы (не допускаются цепи, подключаемые к схеме путем «припаивания» или «накрутки»). Расстояние между линиями схемы должно быть не менее 5 мм.</p> <p>По возможности следует использовать только горизонтальные и вертикальные линии для цепей и компонентов.</p> <p>Высота текста – не менее 3 мм.</p> <p>Рекомендуется минимизировать требования к поступающему на схему питанию (например: переменное напряжение 9 В), размещая на схеме стабилизаторы, аккумуляторы, сетевые фильтры и т.п.</p>
Перечень элементов	Перечень элементов является составной частью принципиальной электрической схемы, что должно быть отражено в нумерации его листов
Алгоритмы функционирования устройства	<p>При выполнении алгоритмов отдельные функции алгоритмов изображаются в виде графических обозначений – символов по ГОСТ 19.003–80.</p> <p>Алгоритм и программу рекомендуется структурировать (разбивать на смысловые блоки); особое внимание уделять разработке программного взаимодействия микропроцессора с компонентами, приведенными в исходных данных задания</p>
Листинги программ	Рекомендуется приводить листинг (результат работы компилятора), а не исходный текст программы

## 1.1. Примерная тематика проектов

Тематика курсовых проектов предполагает разработку продуктов и/или систем ИКТ в защищенном исполнении, аппаратно-программных и/или программных комплексов (сервисов ИБ), реализующих законченную группу механизмов обеспечения ИБ или аппаратно-программное средство для контроля и управления ИБ на объекте информатизации. При этом следует иметь в виду, что защита информации в системах ИКТ и автоматизированных системах (АС) обеспечивается применением комплекса аппаратных, аппаратно-программных, программных средств защиты и проведением организационных мероприятий, составляющих систему защиты информации объекта информатизации.

В задании по курсовому проектированию в соответствии с СТБ 34.101.9 и СТБ 34.101.10 указываются требования к системе защиты информации (СЗИ) в системе ИКТ или АС объекта информатизации, которые приводятся в следующих разделах технического задания (ТЗ) на создание АС по ГОСТ 34.602:

- назначение и цели создания (развития) системы;
- характеристика объектов информатизации;
- политика безопасности организации и требования к СЗИ;
- состав и содержание работ по созданию системы;
- порядок контроля и приемки системы;
- требования к составу и содержанию работ по подготовке объекта информатизации к вводу системы в действие;
- требования к документированию;
- источники разработки.

Требования к СЗИ могут задаваться путем установления требования ее соответствия выбранному профилю защиты по СТБ 34.101.1. В этом случае в разделах ТЗ конкретизируют требования, приведенные в профиле защиты, а также приводят дополнительные требования.

Для объектов курсового проектирования, исполнение которых предусматривает разработку аппаратно-программного комплекса (сервиса безопасности) в ТЗ указываются общие требования, предъявляемые к аппаратной и программной части комплексов РЭА общего назначения и специальные требования к механизмам защиты ин-

формации, реализуемым этим комплексом. Задание по безопасности при этом не разрабатывается, а разрабатывается профиль защиты поддерживающих программных средств, например, «Профиль защиты программных средств межсетевое экрана для организации демилитаризованной зоны корпоративной сети».

## 1.2. Разработка технического задания

Техническое задание должно иметь титульный лист, оформленный в соответствии с образцом, представленным на рис. 1.1.

<p style="text-align: center;"><b>Белорусский национальный технический университет</b> Приборостроительный факультет Кафедра «Информационно-измерительная техника и технологии»</p> <p style="text-align: center;"><i>(Тема проекта)</i></p> <p style="text-align: center;"><b>ТЕХНИЧЕСКОЕ ЗАДАНИЕ</b></p> <p>Исполнитель: студент (факультет, курс, группа)</p> <p>_____</p> <p style="text-align: center;">(фамилия, имя, отчество)</p> <p>Руководитель проекта _____</p> <p>(ученое звание, ученая степень, должность)</p> <p>_____</p> <p style="text-align: center;">(фамилия, имя, отчество)</p> <p style="text-align: center;"><b>Минск 20__</b></p>
---

Рис. 1.1. Титульный лист технического задания

Техническое задание должно включать следующие разделы:

**1. Наименование и область применения (использования) системы или продукта.** Описывается, где и для чего может применяться проектируемая система или продукт ИКТ, например:

*1. Защищенная система организации проведения электронных тендерных торгов предназначена для проведения оптовой торговли продукцией (сырьем) в системе товарно-сырьевых бирж.*

2. Межсетевой экран экспертного класса предназначен для организации демилитаризованных и доверенных зон в сетях провайдеров информационных услуг и в центрах обработки данных.

2. **Разработчик** студент гр. \_\_\_\_\_ Фамилия Имя Отчество.

3. **Основание для разработки:** задание по курсовому проекту от... (указывается дата утверждения задания).

#### 4. Технические требования.

4.1. **Требования назначения.** Описываются основные технические характеристики системы или продукта (изделия), которые должны быть учтены при разработке проекта. Все числовые характеристики (кроме счетных величин) должны задаваться с допуском: «от... до...», «не более», «не менее» или « $X \pm Y$ », например:

1. Изделие рассчитано на непрерывную круглосуточную работу и применяется в закрытых помещениях жилых и производственных зданий и сооружений автономно или совместно с оборудованием средств вычислительной техники.

Питание от сети переменного тока частотой 50 Гц, напряжением  $220 В \pm 10 \%$ .

Пределы рабочей температуры – от 0 до +70 °С.

Пределы температуры хранения – от -50 до +70 °С.

Влажность – от 10 до 90 %.

Интерфейсы:

Gigabit Ethernet – 2 порта;

10/100BASE-TX – 4 порта.

Количество модульных слотов – 6.

2. Система «Организация электронных тендерных торгов...» рассчитана на эксплуатацию в составе инфраструктуры распределения открытых ключей (PKI X.509).

Система обеспечивает:

1) одновременную обработку заявок (транзакций) – до 100 тысяч;

2) агрегацию широкополосного доступа операторского класса: до 56000 сессий на систему;

3) отражение следующих видов атак:

– sniffеры пакетов;

– IP-спуфинг;

– отказ в обслуживании (DoS, DDoS);

– man-in-the-middle («человек посередине»);

– на уровне приложений;

- сетевую разведку;
- злоупотребление доверием;

- переадресацию портов;
- несанкционированный доступ;
- вирусы и приложения типа «троянский конь».

**4.2. Требования совместимости.** Оговаривается возможность совместной работы проектируемой системы (устройства) с другими устройствами и системами, например:

*Система имеет возможность работать как автономно, так и в составе других систем, имеющих интегрированный интерфейс управления на основе протокола SNMP.*

**4.3. Требования к взаимозаменяемости и унификации.** Задаются в общем виде, например:

*Система или изделие должно иметь следующие возможности:*

- взаимозаменяемость с изделиями той же серии;
- задание новых режимов работы системы для изделий или систем других производителей должно производиться путем внутрисистемной инсталляции.

**4.4. Условия эксплуатации (использования), требования к техническому обслуживанию и ремонту (при необходимости).** Указываются (с допусками) числовые значения влияющих факторов, например:

- 1) напряжение питания – от 3 до 5,5 В;
- 2) ток потребления в режиме индикации времени – не более 20 мА;
- 3) ток потребления в режиме звуковой сигнализации – не более 50 мА;
- 4) изделие должно выдерживать условия эксплуатации, соответствующие умеренно-холодному климату:
  - влажность до 95 %;
  - диапазон рабочих температур – от –20 до +40 °С.

**4.5. Экономические показатели.** Описываются обобщенно, поскольку в проекте не рассчитываются, например:

*Стоимость разработки должна быть минимальна.*

**5. Стадии и этапы разработки.** Указываются в соответствии с заданием по курсовому проектированию, например:

1. *Формулировка технического задания* 20.09.2011 г.
2. *Обзор литературы* 25.09.2011 г.

3. Выбор элементной базы  
(для аппаратно-программных комплексов) 01.10.2011 г.

4. Схемотехническая часть  
(для аппаратно-программных комплексов) 25.10.2011 г.

5. Программная часть  
(для аппаратно-программных комплексов) 05.11.2011 г.

6. Расчетно-пояснительная записка  
(для аппаратно-программных комплексов) 30.11.2011 г.

7. Графический материал 15.12.2011 г.

Для курсовых проектов, носящих характер системных проектов, стадии и этапы разработки задаются в следующем виде:

1. Формулировка технического задания 20.09.2011 г.

2. Обзор литературы 25.09.2011 г.

3. Разработка профиля защиты  
(задания по безопасности) 01.10.2011 г.

4. Разработка проекта верхнего  
(нижнего) уровня 25.10.2011 г.

5. Разработка спецификации сервисов  
безопасности 05.11.2011 г.

6. Оценка достигнутого уровня  
Защищенности 30.11.2011 г.

7. Графический материал 15.12.2011 г.

## 2. ВЫПОЛНЕНИЕ СХЕМ КУРСОВОГО ПРОЕКТА

Схемы выполняют без соблюдения масштаба и действительного пространственного расположения составных частей изделия. Необходимое количество разрабатываемых типов схем проектируемого изделия, а также количество схем каждого типа определяется разработчиком в зависимости от особенностей изделия. Комплект схем должен быть по возможности минимальным, но содержать сведения в объеме, достаточном для проектирования, изготовления, эксплуатации и ремонта изделия. Схему разрешается выполнять на нескольких листах.

В зависимости от видов элементов и связей, входящих в состав изделия, схемы имеют следующие *буквенные коды* (табл. 2.1).



Таблица 2.1

## Буквенные коды

Вид схемы	Буквенный код схемы
Электрические	Э
Гидравлические	Г
Пневматические	П
Газовые (кроме пневматических)	Х
Кинематические	К
Вакуумные	В
Оптические	Л
Деления	Е
Комбинированные	С

Под *комбинированной* схемой понимается один конструкторский документ, на котором выполнены схемы двух или более видов, выпущенные на одно изделие. Например, схема электрогидравлическая.

В зависимости от основного назначения типы схем имеют следующие *цифровые коды* (табл. 2.2).

Таблица 2.2

## Цифровые коды

Тип схемы	Цифровой код схемы
Структурные	1
Функциональные	2
Принципиальные (полные)	3
Соединений (монтажные)	4
Подключения	5
Общие	6

Расположения	7
Объединенные	0

Код схемы состоит из буквы, определяющей вид схемы, и цифры, обозначающей тип схемы, например, Э3 – схема электрическая принципиальная, Э4 – схема электрическая соединений.

Схемы электрические должны изображаться согласно требованиям ЕСКД: ГОСТ 2.743–82, 2.708–81, 2.701–84 и т.д.

*Объединенная* схема в одном конструкторском документе совмещает схемы двух или нескольких типов, выпущенные на одно устройство, например, схема структурная, принципиальная и соединений.

Допускается разрабатывать *совмещенные* схемы, когда схемы одного типа содержат сведения, характерные для схемы другого типа, например, на схеме соединений изделия показывают его внешние подключения.

При необходимости допускается разрабатывать схемы прочих типов. К схемам выпускают в виде самостоятельных документов *таблицы*, содержащие сведения о расположении устройств, соединениях, местах подключения и др. Таким документам присваивают код, состоящий из буквы Т и кода соответствующей схемы. Например, код таблицы соединений к электрической принципиальной схеме – ТЭ3.

Полное обозначение схемы на изделие, например, электрической функциональной, имеет следующий вид: **АБВГ ХХХХХХ.ХХХ Э2**.

## 2.1. Структурная схема устройства

Структурная и функциональная *схемы* является первой моделью электронного устройства. Структурная схема определяет основные функциональные части изделия, их назначение и взаимосвязи. *Структурные* схемы разрабатывают при проектировании изделий (установок) на стадиях, предшествующих разработке схем других типов. Их используют для общего ознакомления с изделием. Достоинством структурной схемы при изучении ЭУ является то, что по ней можно быстро получить представление о составе, структуре и выполняемой им функции (функциях), не обращая внимания на схемную реализацию его функциональных частей.

## 2.2. Функциональная схема устройства

Схема электрическая *функциональная* является одним из основных чертежей проекта, который служит для разъяснения процессов, протекающих в отдельных функциональных цепях изделия, дает детальное представление о работе устройства в целом и отображает все цепи, задействованные для передачи цифровых и аналоговых сигналов. На линиях взаимосвязи рекомендуется стрелками указывать направления действия сигналов или потоков энергии. Такие схемы используют для изучения принципов работы изделий (установок), а также при их наладке, контроле и ремонте в процессе эксплуатации.

Графическое построение схемы должно давать наиболее наглядное представление о последовательности взаимодействия функциональных частей устройства. При этом в основных полях УГО опускаются наименования компонентов, т.к. на этом этапе разработки они еще не определены. Опускаются цифры, обозначающие номера выводов микросхем.

При разработке схемы устройства основное внимание уделяется сопряжению микроконтроллера с первичным преобразователем, исполнительными устройствами и заданным интерфейсом. Такие вопросы, как разработка и расчет источника питания или экономическая целесообразность выбора той или иной элементной базы в данном курсовом проекте являются второстепенными, и при необходимости для них могут быть использованы типовые решения без подтверждения расчетами. В то же время параметры основной части схемы, обеспечивающей сопряжение ее основных элементов и узлов, и в особенности метрологические характеристики устройства, должны быть в обязательном порядке обоснованы расчетом либо ссылкой на справочную литературу.

## 2.3. Схема электрическая принципиальная

Схема электрическая *принципиальная* является основным чертежом проекта, по которому в дальнейшем изготавливаются чертежи печатных плат и, в конечном счете, само устройство. Принципиальная схема определяет полный состав элементов и связей между ними и дает детальное представление о принципах работы изделия.

Все микросхемы и электронные компоненты должны изображаться в виде условных графических обозначений (рис. 2.1).

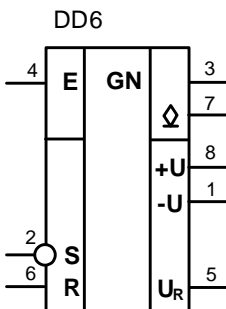


Рис. 2.1. Стиль изображения микросхем

По возможности линии связи объединяются в *шины*. Рекомендуется формировать шины в соответствии с функциональным назначением цепей. Если необходимо подчеркнуть назначение шин, они могут именоваться. Линии связи, входящей в шину, присваивается уникальный в пределах шины числовой номер. Вместо цифр могут использоваться буквы или функциональное назначение линии. Отводы линий могут быть выполнены не только под прямым углом, но и с наклоном, кратным  $45^\circ$ . В этом случае направление примыкания указывает на направление прохождения данной линии в линии групповой связи. Если на групповой линии имеется короткая косая засечка, то цифра рядом с ней отображает число линий в групповой линии, или разрядность цифровой шины (рис. 2.2).

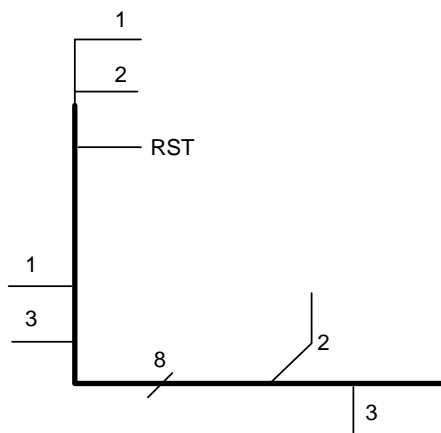


Рис. 2.2. Линия групповой связи (шина)

Минимальное расстояние между соседними линиями, отходящими от групповой в разные стороны, должно быть не менее 2 мм. Линии, выходящие из конца линии групповой связи, изображают линиями нормальной толщины.

## 2.4. Схемы монтажные, подключения, расположения

Схема *соединений (монтажная)* показывает соединения составных частей изделия (установки) и определяет провода, жгуты, кабели, которыми осуществляются эти соединения, а также места их присоединений и ввода (разъемы, платы, зажимы и т.п.). Схематическими соединениями пользуются при разработке чертежей, определяющих прокладку и способы крепления проводов, жгутов, кабелей или трубопроводов в изделии. Схемы используют также при контроле, эксплуатации и ремонте изделий (установок) в процессе эксплуатации.

Схема *подключения* показывает внешние подключения изделия. Схематическими подключениями пользуются при разработке других конструкторских документов, а также для осуществления подключений изделий и при их эксплуатации. Общая схема определяет составные части комплекса и соединения их между собой на месте эксплуатации. Схематическими подключениями пользуются при ознакомлении с комплексами, а также при их контроле и эксплуатации.

Схема *расположения* определяет относительное расположение составных частей устройства, а при необходимости также проводов,

жгутов, кабелей, трубопроводов и т.п. Схемами расположения пользуются при разработке других конструкторских документов, а также при эксплуатации и ремонте.

## 2.5. Выполнение блок-схемы алгоритма программы

Правила выполнения схем алгоритмов, программ, данных и систем регламентируются ГОСТ 19.701–90 «Единая система программной документации. Схемы алгоритмов, программ, данных и систем. Условные обозначения и правила выполнения».


Схемы программ (алгоритмов программ) отображают последовательность операций в программе.


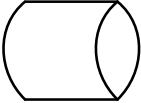

Схема программы состоит:

- 1) из символов процесса, указывающих фактически операции обработки данных (включая символы, определяющие путь, которого следует придерживаться с учетом логических условий);
- 2) линейных символов, указывающих поток управления;
- 3) специальных символов, используемых для облегчения написания и чтения схемы (табл. 2.3).




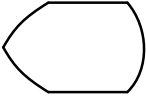
Таблица 2.3




### Оформление элементов блок-схемы

Обозначение	Наименование	Функция
Символы данных		
	Данные	Отображает данные, носитель данных не определен
	Запоминаемые данные	Отображает хранимые данные в виде, пригодном для обработки, носитель данных не определен
	Оперативное запоминающее устройство	Отображает данные, хранящиеся в оперативном запоминающем устройстве

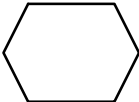
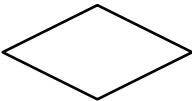
	Запоминающее устройство с последовательным доступом	Отображает данные, хранящиеся в запоминающем устройстве с последовательным доступом (магнитная лента, кассета с магнитной лентой, магнитофонная кассета)
	Запоминающее устройство с прямым доступом	Отображает данные, хранящиеся в запоминающем устройстве с прямым доступом (магнитный диск, магнитный барабан, гибкий магнитный диск)
	Документ	Отображает данные, представленные на носителе в удобочитаемой форме (машинограмма, документ для оптического или магнитного считывания, микрофильм, рулон ленты с итоговыми данными, бланки ввода данных)

Продолжение табл. 2.3

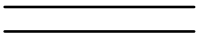
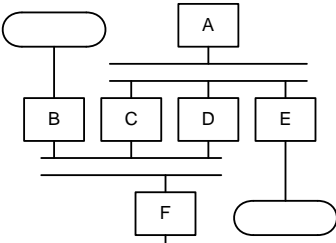
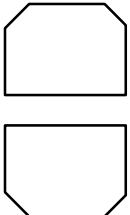
Обозначение	Наименование	Функция
	Ручной ввод	Отображает данные, вводимые вручную во время обработки с устройств любого типа (клавиатура, переключатели, кнопки, световое перо, полоски со штриховым кодом)
	Карта	Отображает данные, представленные на носителе в виде карты (перфокарты, магнитные карты, карты со считываемыми метками, карты с отрывным ярлыком, карты со сканируемыми метками)
	Бумажная лента	Отображает данные, представленные на носителе в виде бумажной ленты
	Дисплей	Отображает данные, представленные в человекочитаемой форме на носителе в виде отображающего устройства (экран для визуального наблюдения, индикаторы ввода информации)
Символы процесса		

	<p>Процесс</p>	<p>Отображает функцию обработки данных любого вида (выполнение определенной операции или группы операций, приводящее к изменению значения, формы или размещения информации или к определению того, по какому из нескольких направлений потока следует двигаться)</p>
	<p>Предопределенный процесс</p>	<p>Отображает предопределенный процесс, состоящий из одной или нескольких операций или шагов программы, которые определены в другом месте (в подпрограмме, модуле)</p>
	<p>Ручная операция</p>	<p>Отображает любой процесс, выполняемый человеком</p>

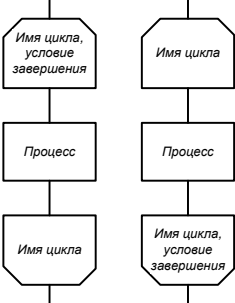

Продолжение табл. 2.3




Обозначение	Наименование	Функция
	<p>Подготовка</p>	<p>Отображает модификацию команды или группы команд с целью воздействия на некоторую последующую функцию (установка переключателя, модификация индексного регистра или инициализация программы)</p>
	<p>Решение</p>	<p>Отображает решение или функцию переключательного типа, имеющую один вход и ряд альтернативных выходов, один и только один из которых может быть активизирован после вычисления условий, определенных внутри этого символа. Соответствующие результаты вычисления могут быть записаны по соседству с линиями, отображающими эти пути</p>



	<p>Параллельные действия</p>	<p>Отображает синхронизацию двух или более параллельных операций</p> <p><i>Пример:</i></p> 
	<p>Граница цикла</p>	<p>Состоит из двух частей. Отображает начало и конец цикла. Обе части символа имеют один и тот же идентификатор. Условия для инициализации, приращения, завершения и т.д. помещаются внутри символа в начале или в конце в зависимости от расположения операции, проверяющей условие</p>

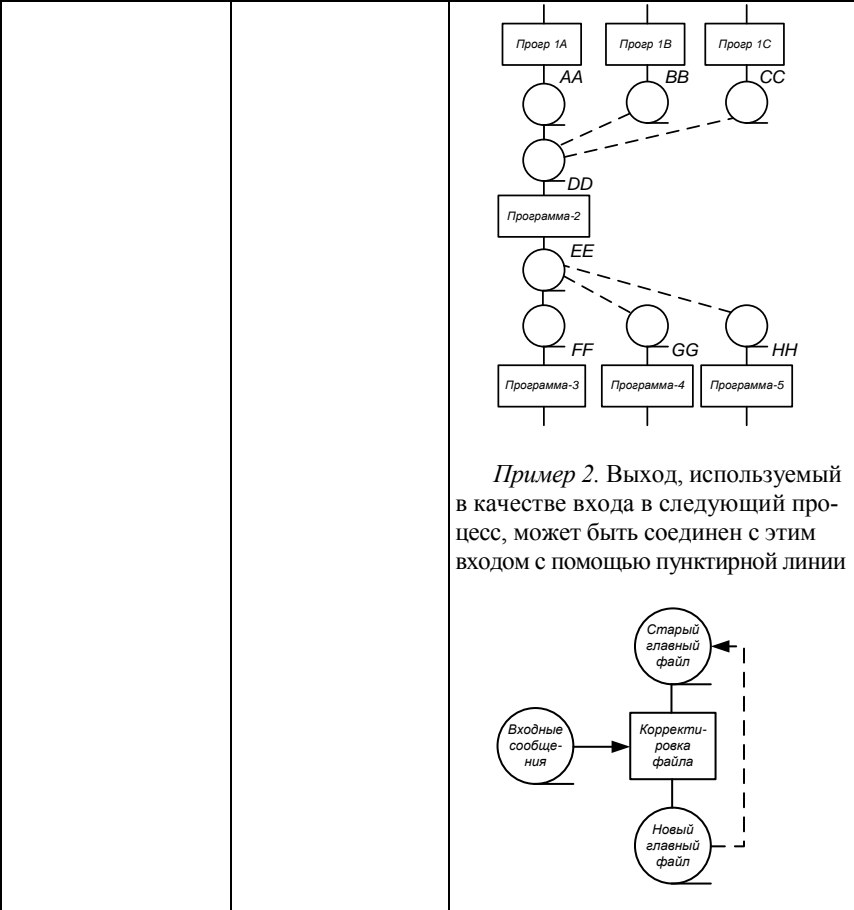
Продолжение табл. 2.3

Обозначение	Наименование	Функция
		<p><i>Пример 1:</i>      <i>Пример 2:</i></p> 
Символы линий		
	<p>Линия</p>	<p>Отображает поток данных или управления.</p> <p>При необходимости для повышения удобочитаемости могут быть добавлены стрелки-указатели</p>


	<p>Передача управления</p>	<p>Отображает непосредственную передачу управления от одного процесса к другому, иногда с возможностью прямого возвращения к инициирующему процессу после того, как инициированный процесс завершит свои функции. Тип передачи управления должен быть назван внутри символа (например, запрос, вызов, событие)</p>
	<p>Канал связи</p>	<p>Отображает передачу данных по каналу связи</p>
	<p>Пунктирная линия</p>	<p>Отображает альтернативную связь между двумя или более символами. Кроме того, символ используют для обведения аннотированного участка. <i>Пример 1.</i> Если один из ряда альтернативных выходов используют в качестве входа в процесс, либо когда выход используется в качестве входа в альтернативные процессы, эти символы соединяют пунктирными линиями</p>

Продолжение табл. 2.3

Обозначение	Наименование	Функция
-------------	--------------	---------

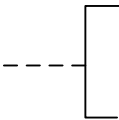
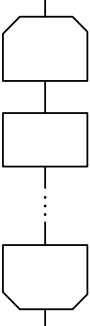


Специальные символы

	<p>Соединитель</p>	<p>Отображает выход в часть схемы и вход из другой части этой схемы и используется для обрыва линии и продолжения ее в другом месте. Соответствующие символы-соединители должны содержать одно и то же уникальное обозначение</p>
---	--------------------	---

Окончание табл. 2.3

Обозначение	Наименование	Функция
-------------	--------------	---------

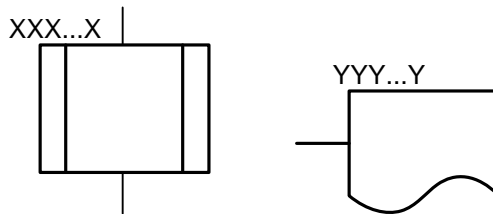
	<p>Терминатор</p>	<p>Отображает выход во внешнюю среду и вход из внешней среды (начало или конец схемы программы, внешнее использование и источник или пункт назначения данных)</p>
	<p>Комментарий</p>	<p>Используется для добавления описательных комментариев или пояснительных записей в целях объяснения или примечаний. Пунктирные линии в символе комментария связаны с соответствующим символом или могут обводить группу символов. Текст комментариев или примечаний должен быть помещен около ограничивающей фигуры</p>
	<p>Пропуск</p>	<p>Используется в схемах для отображения пропуска символа или группы символов, в которых не определены ни тип, ни число символов. Применяется только в символах линии или между ними. Он используется главным образом в схемах, изображающих общие решения с неизвестным числом повторений</p> <p><i>Пример:</i></p> 

*Правила применения символов*

Символы могут быть вычерчены в любой ориентации, но предпочтительной является горизонтальная. Зеркальное изображение формы символа обозначает одну и ту же функцию, но не является предпочтительным. Минимальное количество текста, необходимого для понимания функции символа, следует помещать внутри этого символа. Текст для чтения должен записываться слева направо и сверху вниз независимо от направления потока. Если объем текста, помещаемого внутри символа, превышает его размеры, следует использовать символ комментария.

В схемах может использоваться идентификатор символов. Это связанный с данным символом идентификатор, который определяет символ для использования в справочных целях в других элементах документации (например, в листинге программы). Идентификатор символа должен располагаться слева над символом.

*Пример:*



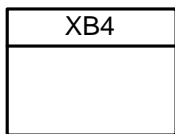
В схемах может использоваться подробное представление, которое обозначается с помощью символа с полосой для процесса или данных. Символ с полосой указывает, что в этом же комплекте документации в другом месте имеется более подробное представление.

Символ с полосой представляет собой любой символ, внутри которого в верхней части проведена горизонтальная линия. Между этой линией и верхней линией символа помещен идентификатор, указывающий на подробное представление данного символа.

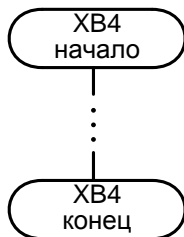
В качестве первого и последнего символа подробного представления должен быть использован символ указателя конца. Первый символ указателя конца должен содержать ссылку, которая имеется также в символе с полосой.

*Пример:*

Символ с полосой



Подробное представление



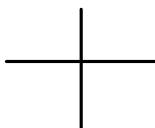
### *Правила выполнения соединений*

Потоки данных или потоки управления в схемах показываются линиями. Направление потока слева направо и сверху вниз считается стандартным.

В случаях, когда необходимо внести большую ясность в схему (например, при соединениях), на линиях используются стрелки. Если поток имеет направление, отличное от стандартного, стрелки должны указывать это направление.

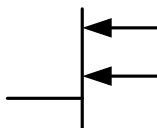
В схемах следует избегать пересечения линий. Пересекающиеся линии не имеют логической связи между собой, поэтому изменения направления в точках пересечения не допускаются.

*Пример:*



Две или более входящие линии могут объединяться в одну исходящую линию. Если две или более линии объединяются в одну линию, место объединения должно быть смещено.

*Пример:*



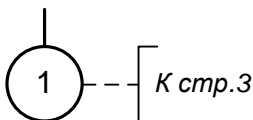
Линии в схемах должны подходить к символу либо слева, либо сверху, либо сверху, а исходить либо справа, либо снизу. Линии должны быть направлены к центру символа.

При необходимости линии в схемах следует разрывать для избежания излишних пересечений или слишком длинных линий, а также если схема состоит из нескольких страниц. Соединитель в начале разрыва называется внешним соединителем, а соединитель в конце разрыва – внутренним соединителем.

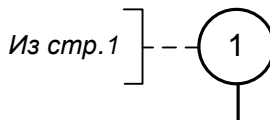
Ссылки к страницам могут быть приведены совместно с символом комментария для их соединителей.

*Пример:*

Внешний соединитель



Внутренний соединитель

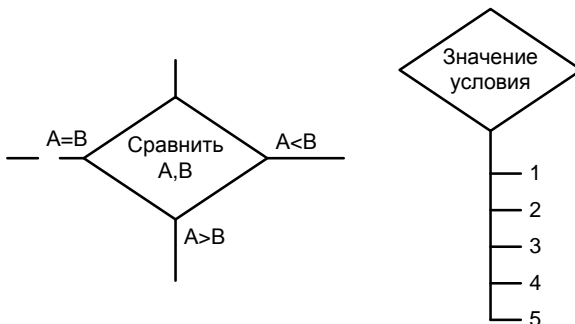


Несколько выходов из символа следует показывать:

- 1) несколькими линиями от данного символа к другим символам;
- 2) одной линией от данного символа, которая затем разветвляется в соответствующее число линий.

Каждый выход из символа должен сопровождаться соответствующими значениями условий, чтобы показать логический путь, который он представляет, с тем, чтобы эти условия и соответствующие ссылки были идентифицированы.

*Примеры:*



## 2.6. Выполнение функциональных схем проекта верхнего и/или нижнего уровня

Графические (символьные) изображения функциональных подсистем систем ИКТ и объектов информатизации в отечественной нормативной базе отсутствуют. Из этих соображений при выполнении функциональных схем проектов верхнего и/или нижнего уровня следует руководствоваться международной (фирменной) символикой. Приведем пример построения такой схемы с использованием международной символики. Данная корпоративная интрасеть состоит из пользовательских компьютеров, серверов, маршрутизаторов и коммутаторов. Обобщенная функциональная схема (модель) корпоративной сети представлена на рис. 2.3.

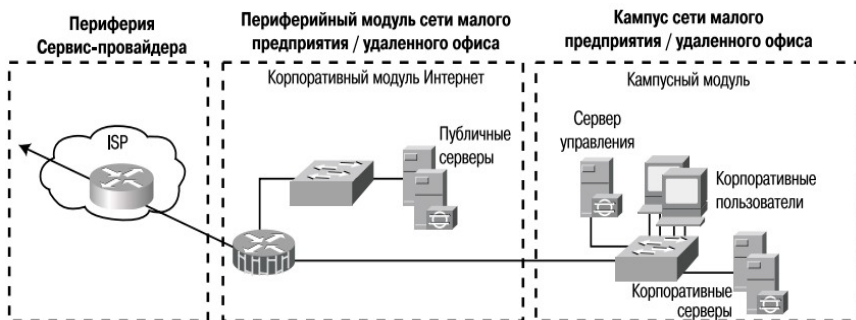




Рис. 2.3. Модель корпоративной интрасети

В табл. 2.4 представлены условные обозначения функциональных узлов и элементов систем ИКТ.

Таблица 2.4

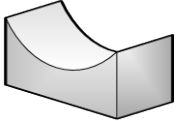


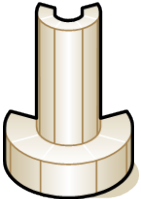
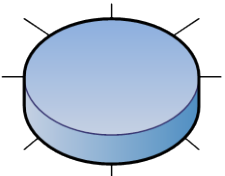
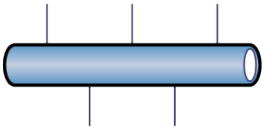

### Условные обозначения

	Маршрутизатор
	Маршрутизатор с функциями межсетевоего экрана



Продолжение табл. 2.4

	<p>Коммутатор уровня 2</p>
	<p>Рабочая станция</p>
	<p>Коммуникационный сервер</p>
	<p>Терминальный сервер</p>
	<p>Сервер выдачи цифровых сертификатов</p>
	<p>Сервер выдачи открытых ключей</p>
	<p>Межсетевой экран (<i>Firewall</i>)</p>

	<p>Мост или концентратор</p>
	<p>Сервер</p>
	<p>Компьютер типа <i>Mainframe</i></p>
	<p>Суперкомпьютер</p>
	<p>Сеть кольцевой топологии</p>
	<p>Сеть шинной топологии</p>
	<p>Коммутируемое подключение</p>

	Точка доступа к радиосети
	Модем
	Пользователь

## 2.7. Разработка профиля защиты

### 2.7.1. Общие положения

Профиль защиты (ПЗ) определяет совокупность требований безопасности для типовых объектов ИТ. Такие объекты отвечают общим требованиям безопасности ИТ, предъявляемым заказчиками (потребителями). Это дает возможность заказчикам (потребителям) задавать требования в части безопасности ИТ на основе существующих ПЗ или создавать новые.

В настоящем методическом пособии рассматриваются требования к содержанию структурных элементов ПЗ. Эти требования содержатся в гарантийном классе АРЕ «Оценка профиля защиты» СТБ 34.101.3 в виде гарантийных компонентов, которые должны использоваться при оценке ПЗ.

### 2.7.2. Содержание профиля защиты

#### *Содержание и представление*

Содержание ПЗ должно отвечать требованиям настоящего документа. ПЗ представляется в виде документа, предназначенного для

пользователя ПЗ и имеющего минимальное число ссылок на другие источники с тем, чтобы облегчить его изучение. Если необходимо, то отдельно может представляться обоснование ПЗ.

Структура ПЗ представлена на рис. 2.4. Она может быть использована при разработке структурных элементов ПЗ.



Рис. 2.4. Структура профиля защиты

### *Введение в описание профиля защиты*

Введение в описание ПЗ должно содержать руководство по использованию документа и обзор информации, необходимой для работы с регистром ПЗ. Оно включает:

а) идентификацию ПЗ, которая должна представлять описательную информацию, необходимую для идентификации, каталогизации, регистрации и ссылок в ПЗ;

б) обзор ПЗ, который должен представлять краткое описание ПЗ. Обзор должен быть достаточно подробным, чтобы потенциальный пользователь ПЗ, прочитав его, мог составить заключение о пригодности ПЗ для его целей. Обзор должен быть также удобным для представления в виде самостоятельного реферата в каталогах и регистрах ПЗ.

### *Описание объекта*

Описание объекта должно способствовать формулированию требований безопасности и давать представление о типе продукта и его общих характеристиках.

Описание объекта представляет данные для его оценки, но само описание не оценивается. Информацию, содержащуюся в описании объекта, можно использовать в процессе оценки для выявления несоответствий между политикой, задачами и требованиями безопасности объекта. Поскольку ПЗ не относится к конкретной реализации, параметры объекта могут быть описаны на основании предположений. Если объект является продуктом или системой, основной функцией которых является безопасность, то этот раздел можно использовать для описания более широкого круга возможных областей применения объекта.

### *Среда безопасности объекта*

Описание среды безопасности объекта должно содержать связанные с безопасностью характеристики среды, в которой будет использоваться объект, и предполагаемый способ его эксплуатации. Оно включает:

1) предположения, которые должны содержать следующие связанные с безопасностью характеристики среды объекта:

– информацию о предполагаемом использовании объекта, в том числе о прикладной области применения, предполагаемой стоимости активов и о возможных ограничениях на использование;

– информацию о среде, в которой будет использоваться объект, включая вопросы, связанные с комплексом средств безопасности

объекта оценки (КСБО), подбором персонала и внешними связями с другими объектами;

2) угрозы активам, которые исходят из окружающей среды объекта и создают опасность для его работы и против которых требуется защита средствами объекта и его среды.

Угрозы должны быть описаны в понятиях: источник угроз (нарушитель), атака и актив, который подвергается атакам; источники угроз – в следующих понятиях: квалификация, используемый ресурс и мотивация; атаки – в понятиях: методы атак, используемые уязвимые места и возможности для атаки.

Если задачи безопасности объекта выводятся только из политики безопасности организации и предположений, то структурный элемент «Угрозы» можно опустить;

3) политику безопасности организации, которая должна определять и при необходимости объяснять разделы политики безопасности или правила, которым должен соответствовать объект. Каждый раздел политики следует представлять в форме, позволяющей использовать ее для формулирования четких задач безопасности ИТ.

Если задачи безопасности объекта выводятся только из угроз и предположений, то структурный элемент «Политика безопасности организации» можно опустить.

Для территориально разнесенного объекта анализ среды безопасности объекта (предположений, угроз, политики безопасности) должен производиться отдельно для каждого района расположения объекта и условий его эксплуатации.

### *Задачи безопасности*

Задачи безопасности должны отражать намерение противостоять всем установленным угрозам и/или поддерживать принятую политику безопасности и предположения. Различают следующие типы задач безопасности:

а) задачи безопасности для объекта, которые должны быть четко сформулированы для того, чтобы их реализация позволила противостоять угрозам средствами безопасности объекта и/или поддерживать политику безопасности организации, которой должен следовать объект;

б) задачи безопасности для среды, которые должны быть четко сформулированы для того, чтобы их решение позволило противостоять угрозам средствами безопасности объекта и среды и/или поддерживать политику безопасности организации, которой должен следовать объект. Формулировки задач безопасности для среды могут повторять (частично или полностью) предположения в описании среды безопасности объекта.

*Примечание.* Если противодействие угрозе или проведение политики безопасности возлагается на объект и его среду, то соответствующие задачи безопасности формулируются для объекта и среды.

### *Требования безопасности информационных технологий*

Требования безопасности ИТ должны задаваться следующим образом:

1. В разделе «Требования безопасности объекта» представляются функциональные и гарантийные требования безопасности, которым должен отвечать объект, и заключение о соответствии требований задачам безопасности объекта.

Требования безопасности объекта включают в себя:

1) функциональные требования безопасности объекта, которые должны задаваться как функциональные компоненты по СТБ 34.101.2.

В тех случаях, когда по условиям безопасности требуется выделить различные аспекты одного и того же требования (например, при идентификации нескольких типов пользователей), можно повторно (т.е. применив операцию итерации) использовать один и тот же компонент.

Если гарантийные требования объекта включают компонент AVA\_SOF.1 «Оценка стойкости средства обеспечения безопасности», то в описании функциональных требований безопасности объекта должен устанавливаться минимальный уровень стойкости для средств безопасности (СБ), реализованных вероятностными методами или методами перестановок (например, с помощью паролей или хэш-функций). Все эти средства должны обладать по крайней мере этим уровнем стойкости. Имеется три уровня стойкости средств безопасности: базовый, средний и высокий. Выбор уровня стойкости производится в соответствии с задачами безопасности объекта. При решении определенных задач безопасности допуска-

ется для реализации некоторых функциональных требований выбирать специальную меру стойкости СБ.

При выборе уровня стойкости СБ (компонент AVA\_SOF.1 «Оценка стойкости средства обеспечения безопасности») необходимо установить, соответствуют ли выбранные уровни стойкости отдельных СБ и объекта в целом общему минимальному уровню стойкости;

2) гарантийные требования безопасности объекта, которые должны задаваться в виде одного из УГО, возможно, усиленного за счет гарантийных компонентов по СТБ 34.101.3. Усиление УГО в ПЗ может осуществляться также за счет включения в ПЗ дополнительных гарантийных компонентов, не входящих в СТБ 34.101.3.

2. В разделе «Требования безопасности для среды ИТ» содержатся требования безопасности, которым должна соответствовать среда ИТ объекта. Если объект независим от среды ИТ, то этот раздел можно опустить. Требования безопасности, не относящиеся к среде ИТ, но часто используемые на практике, могут не включаться в ПЗ, так как они не связаны непосредственно с реализацией объекта.

3. Перечисленные ниже условия формирования требований безопасности в равной степени относятся как к функциональным и гарантийным требованиям безопасности объекта, так и к его среде:

1) требования безопасности ИТ должны быть представлены в виде компонентов требований безопасности по СТБ 34.101.2 и СТБ 34.101.3. Если компоненты требований безопасности по СТБ 34.101.2 и СТБ 34.101.3 не применимы для проектирования ПЗ типового объекта или этих компонентов недостаточно, то недостающие требования безопасности задаются независимо от компонентов требований по СТБ 34.101.2 и СТБ 34.101.3;

2) дополнительные функциональные и гарантийные требования безопасности должны быть четко и однозначно сформулированы, чтобы не возникало трудностей при их оценке и проверке степени их реализации. Образцом уровня детализации и способа представления требований безопасности может стать представление функциональных или гарантийных требований по СТБ 34.101.2 и СТБ 34.101.3;

3) в ПЗ должны быть включены компоненты требований, в которых предусмотрены операции назначения и выбора. Тем самым обеспечивается соответствие требований задачам безопасности;



4) используя в описании требований безопасности объекта операции назначения и выбора над компонентами требований, можно, где это необходимо, разрешать или запрещать использовать отдельные механизмы безопасности;

5) должны быть удовлетворены зависимости между требованиями безопасности объекта за счет включения дополнительных требований в перечень требований безопасности объекта либо среды.

### *Замечания по применению профиля защиты*

Этот структурный элемент содержит уточняющую информацию и пояснения к операциям, которые в ПЗ не являются завершенными, а также другую информацию о ПЗ, которая может быть полезна при проектировании, разработке, оценке или эксплуатации объекта.

### *Обоснование профиля защиты*

В этом структурном элементе приводится обоснование ПЗ, которое должно подтвердить, что ПЗ является полной и взаимоувязанной совокупностью требований и что соответствующий ему объект будет обладать эффективным набором СБ ИТ в среде безопасности. Он включает:

а) обоснование задач безопасности, которое должно подтвердить, что задачи безопасности охватывают все аспекты безопасности среды использования объекта и вытекают из политики безопасности организации для объекта;

б) обоснование требований безопасности, которое должно подтвердить, что совокупность требований безопасности объекта и его окружающей среды отвечает задачам безопасности.

При обосновании требований безопасности необходимо показать, что:

1) комбинация отдельных компонентов функциональных и гарантийных требований безопасности объекта и его среды обеспечивает решение задач безопасности;

2) набор требований безопасности образует единую и внутренне связную совокупность требований;

3) выбор требований безопасности обоснован. Специальное обоснование необходимо при задании требований, не содержащихся в

СТБ 34.101.2 и СТБ 34.101.3, при задании гарантийных требований, не включенных в УГО, а также в случае неудовлетворенных зависимостей;

4) выбор уровня стойкости комплекса средств обеспечения безопасности обоснован. Требования к стойкости КСБО должны быть согласованы с задачами безопасности объекта оценки.

Обоснование допускается не включать в ПЗ, однако орган по регистрации ПЗ должен обеспечить возможность ознакомления с ним пользователей ПЗ.

## **2.8. Разработка задания по безопасности**

### **2.8.1. Общие положения**

Задание по безопасности (ЗБ) содержит требования безопасности ИТ для конкретного объекта оценки, определяет функциональные и гарантийные меры безопасности, реализация которых обеспечивает соответствие объекта установленным требованиям.

ЗБ является основой для соглашения между разработчиками, экспертами и, если необходимо, заказчиками (потребителями) по характеристикам безопасности объекта и области применения объекта. Лица, заинтересованные в таком задании, не ограничиваются только ответственными за разработку объекта и оценку его безопасности, но к ним также могут быть отнесены ответственные за управление, маркетинг, продажу, установку, конфигурирование, функционирование и использование объекта.

ЗБ может включать набор требований безопасности или условия соответствия одному или нескольким ПЗ.

### **2.8.2. Содержание задания по безопасности**

#### *Содержание и представление*

Содержание ЗБ должно отвечать требованиям настоящего приложения. ЗБ должно быть представлено в виде документа с минимальным количеством ссылок на другие источники, которые могут оказаться недоступными пользователю ЗБ. Если необходимо, то отдельно представляется обоснование ЗБ.

Структура ЗБ приведена на рис. 2.5. Она используется при разработке структурных элементов ЗБ.

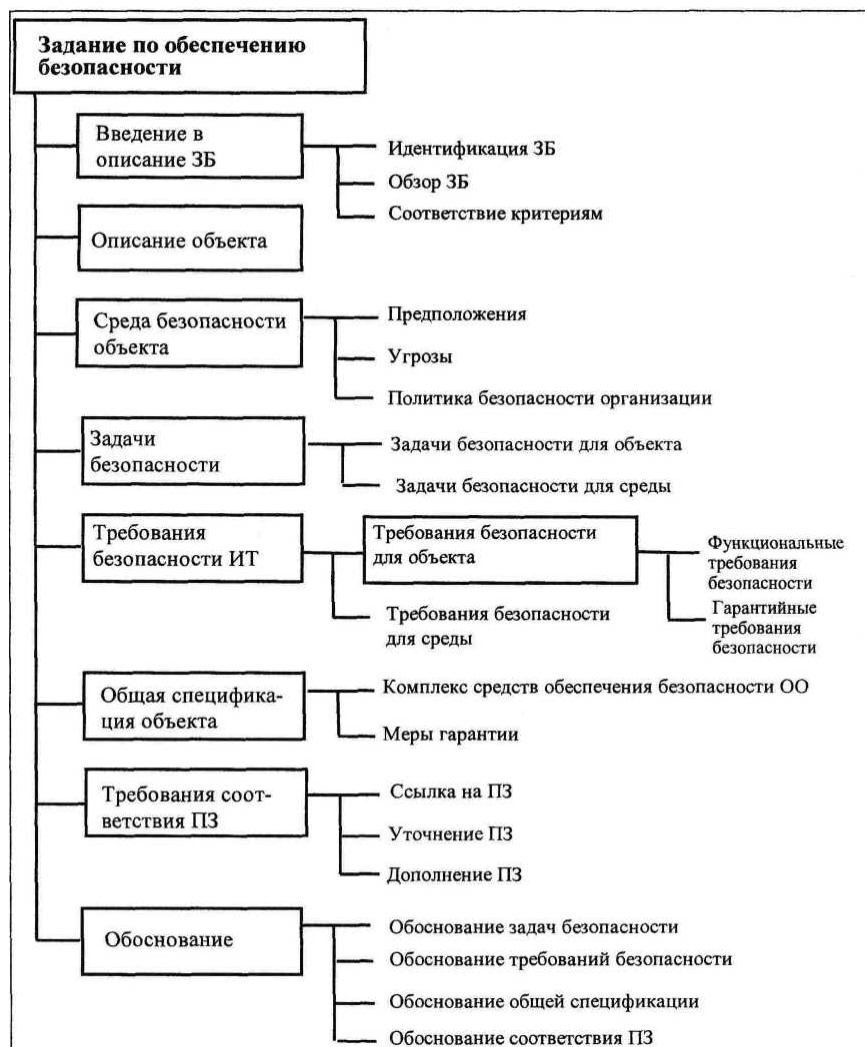


Рис. 2.5. Структура задания по безопасности

## *Введение в описание задания по безопасности*

Введение в описание ЗБ должно включать следующие структурные элементы:

а) идентификацию ЗБ, которая должна содержать обозначения и описания, необходимые для идентификации ЗБ и объекта, к которому оно относится;

б) обзор ЗБ, в котором должно быть представлено краткое описание ЗБ. Обзор должен быть достаточно подробным, чтобы потенциальный потребитель объекта мог составить заключение о пригодности объекта для своих целей. Обзор должен быть также удобным для представления в виде отдельного реферата в перечне сертифицированных продуктов;

в) требования соответствия стандарту, в которых должна быть определена степень достоверности, с которой ЗБ соответствует функциональным, гарантийным требованиям или непосредственно ПЗ типового объекта.

### *Описание объекта*

Описание объекта должно обеспечивать понимание требований его безопасности и давать представление о типе продукта или системы ИТ, а также содержать описание как физических (аппаратных и/или программных компонентов/модулей), так и логических (характеристик ИТ и безопасности объекта) возможностей и областей применения объекта.

Описание объекта представляет данные для его оценки. Информацию, содержащуюся в описании объекта, можно использовать в процессе оценки для выявления несоответствий между политикой, задачами и требованиями безопасности объекта. Если объект представляет продукт или систему, основной функцией которых является безопасность, то этот раздел можно использовать для описания более широкого круга области применения объекта.

### *Среда безопасности объекта*

Описание среды безопасности объекта должно содержать связанные с безопасностью характеристики среды, в которой будет использоваться объект, и предполагаемый способ эксплуатации объекта. Оно включает:

1) предположения, которые должны содержать следующие связанные с безопасностью характеристики среды объекта:

– информацию о предполагаемом порядке использования объекта, в том числе о прикладной области применения, предполагаемой стоимости активов и о возможных ограничениях на использование;

– информацию о среде, в которой будет использоваться объект, включая вопросы, связанные с КСБО, подбором персонала и внешними связями с другими объектами;

2) угрозы активам, которые исходят из окружающей среды объекта и создают опасность для его работы и против которых требуется защита средствами объекта или его среды.

Угрозы должны быть описаны в понятиях: источник угроз (нарушитель), атака и актив, который подвергается атакам; источники угроз – в следующих понятиях: методы атак, используемые уязвимые места и возможности для атаки.

Если задачи безопасности объекта выводятся только из политики безопасности организации и предположений, то структурный элемент «Угрозы» в ЗБ можно опустить;

3) политику безопасности организации, которая должна определять и при необходимости объяснять разделы политики безопасности или правила, которым должен соответствовать объект. Каждый раздел политики следует представлять в форме, позволяющей использовать ее для формулирования четких задач безопасности ИТ.

Если задачи безопасности объекта выводятся только из угроз и предположений, то структурный элемент «Политика безопасности организации» в ЗБ можно опустить.

Для территориально разнесенного объекта анализ среды безопасности объекта (предположений, угроз, политики безопасности) должен производиться отдельно для каждого района расположения объекта и условий его эксплуатации.

### *Задачи безопасности*

Задачи безопасности должны отражать намерение противостоять всем установленным угрозам и/или поддерживать принятую политику безопасности и предположения. Различают следующие типы задач безопасности:

а) задачи безопасности для объекта, которые должны быть четко сформулированы для того, чтобы их решение позволило противостоять угрозам средствами безопасности объекта и/или поддерживать политику безопасности организации, которой должен следовать объект;

б) задачи безопасности для среды, которые должны быть четко сформулированы для того, чтобы их решение позволило противостоять угрозам средствами безопасности объекта и среды и/или поддерживать политику безопасности организации, которой должен следовать объект. Формулировки задач безопасности для среды могут повторять (частично или полностью) предположения в описании среды безопасности объекта.

*Примечание.* Если противодействие угрозе или проведение политики безопасности возлагается на объект и его среду, то соответствующие задачи безопасности формулируются для объекта и среды.

### *Требования безопасности информационных технологий*

Требования безопасности ИТ должны задаваться следующим образом:

1. В разделе «Требования безопасности объекта» представляются функциональные и гарантийные требования безопасности, которым должен отвечать объект, и заключение о соответствии требований задачам безопасности объекта.

Требования безопасности объекта включают в себя:

1) функциональные требования безопасности объекта, которые должны задаваться как функциональные компоненты по СТБ 34.101.2.

В тех случаях, когда по условиям безопасности требуется выделить различные аспекты одного и того же требования (например, при идентификации нескольких типов пользователей), можно повторно (т.е. применив операцию итерации) использовать один и тот же компонент.

Если гарантийные требования объекта включают компонент AVA\_SOF.1 «Оценка стойкости средства обеспечения безопасности», то в описании функциональных требований безопасности объекта должен устанавливаться минимальный уровень стойкости для СБ, реализованных вероятностными методами или методами перестановок (например, с помощью паролей или хэш-функций). КСБО должен обладать по крайней мере этим уровнем стойкости. Имеется

три уровня стойкости СБ: базовый, средний и высокий. Выбор уровня стойкости производится в соответствии с задачами безопасности объекта. При решении определенных задач безопасности допускается для реализации некоторых функциональных требований выбирать специальную меру стойкости СБ.

При выборе уровня стойкости СБ (компонент AVA\_SOF.1 «Оценка стойкости средства обеспечения безопасности») необходимо установить, соответствуют ли выбранные уровни стойкости отдельных СБ и объекта в целом общему минимальному уровню стойкости;

2) гарантийные требования безопасности объекта, которые должны задаваться в виде одного из УГО, возможно, усиленного за счет гарантийных компонентов по СТБ 34.101.3. Усиление УГО в ЗБ может осуществляться также за счет включения дополнительных гарантийных компонентов, не входящих в СТБ 34.101.3;

2. В разделе «Требования безопасности для среды ИТ» содержатся требования безопасности, которым должна соответствовать среда ИТ объекта. Если объект независим от среды ИТ, то этот раздел можно опустить. Требования безопасности, не относящиеся к среде ИТ, но часто используемые на практике, могут не включаться в ЗБ, так как они не связаны непосредственно с реализацией объекта;

3. Перечисленные ниже условия формирования требований безопасности в равной степени относятся как к функциональным и гарантийным требованиям безопасности объекта, так и к его среде:

1) требования безопасности ИТ должны быть представлены в виде компонентов требований безопасности по СТБ 34.101.2 и СТБ 34.101.3. Если компоненты требований безопасности по СТБ 34.101.2 и СТБ 34.101.3 не применимы для ЗБ объекта или этих компонентов недостаточно, то недостающие требования безопасности задаются независимо от компонентов требований по СТБ 34.101.2 и СТБ 34.101.3;

2) дополнительные функциональные и гарантийные требования безопасности должны быть четко и однозначно сформулированы, чтобы не возникало трудностей при их оценке и при проверке степени их реализации. Образцом уровня детализации и способа представления требований безопасности может стать представление функциональных или гарантийных требований по СТБ 34.101.2 и СТБ 34.101.3;

3) должны быть использованы все необходимые операции для конкретизации требований безопасности с тем, чтобы обеспечить

соответствие требований задачам безопасности. Все разрешенные операции над компонентами требований должны быть завершены;

4) должны быть удовлетворены все зависимости между требованиями безопасности объекта. Указанные зависимости могут быть удовлетворены за счет включения необходимых требований в перечень требований безопасности объекта либо среды.

### *Общая спецификация объекта*

Структурный элемент «Общая спецификация объекта» должен содержать описание КСБО и мер гарантии ОО, отвечающих требованиям безопасности. В ряде случаев функциональная информация, являющаяся частью общей спецификации объекта, идентична информации, содержащейся в требованиях семейства ADV\_FSP «Функциональная спецификация».

Общая спецификация объекта включает:

1) описание комплекса средств безопасности объекта, которое должно включать перечень СБ ИТ и определять, каким образом эти средства реализуют функциональные требования безопасности объекта. В описании должно быть взаимное соответствие СБ и требований с четким указанием, какие средства соответствуют каким требованиям, а также подтверждение того, что все требования удовлетворены.

Каждое СБ должно обеспечивать реализацию по крайней мере одного функционального требования безопасности объекта. Это достигается тем, что:

– СБ ИТ определяются неформальным способом на уровне описания, необходимом для понимания их назначения;

– механизмы безопасности должны соответствовать СБ с тем, чтобы можно было определить, какие механизмы безопасности используются для реализации каждого средства;

– если в состав гарантийных требований безопасности объекта входит компонент AVA\_SOF1 «Оценка стойкости средства обеспечения безопасности», то должны быть указаны СБ ИТ, реализованные с помощью вероятностных методов или метода перестановок (например, с помощью пароля или хэш-функции). Возможность нарушения механизма безопасности таких средств посредством преднамеренного или случайного воздействия имеет непосредственное отношение к безопасности объекта. Необходимо провести



анализ стойкости этих средств. Стойкость каждого средства должна быть оценена как базовая, средняя или высокая либо как введенная дополнительно мера стойкости. Результаты оценки стойкости используются экспертом для проверки адекватности и корректности реализации требуемого уровня стойкости;

2) описание мер гарантии, обеспечиваемых установленными гарантийными требованиями. Меры гарантии должны быть отражены таким образом, чтобы было понятно, какие меры участвуют в реализации требований.

Меры гарантии могут быть отражены в ЗБ также путем ссылки на соответствующие планы обеспечения качества, жизненного цикла или управления.

### *Требования соответствия профилям защиты*

В ЗБ может содержаться требование обеспечения соответствия объекта требованиям безопасности одного или нескольких ПЗ. Эта дополнительная часть ЗБ включает разъяснения, подтверждения и иные вспомогательные материалы. Требование соответствия объекта ПЗ может повлиять на форму описания и содержание той части ЗБ, в которой приведены задачи и требования безопасности объекта. Это влияние может быть сведено к следующим случаям:

а) при отсутствии в ЗБ требований на соответствие ПЗ задачи и требования безопасности объекта представляются так, как приведено ранее в соответствующих подпунктах (при этом требования, приведенные в ПЗ, не включаются в ЗБ);

б) при наличии в ЗБ только требований соответствия требованиям безопасности, приведенным в ПЗ, достаточно ссылки на ПЗ, чтобы определить и оценить задачи и требования безопасности объекта (при этом не следует приводить повторно описание ПЗ);

в) если в ЗБ есть требование не только обеспечить соответствие ПЗ, но и провести более глубокую детализацию требований, приведенных в ПЗ, то в ЗБ должно быть показано, что требование детализации удовлетворено.

Такая ситуация обычно возникает, когда ПЗ содержит незавершенные операции. В этом случае в ЗБ может быть сделана ссылка на ПЗ, но дополнительные детализированные требования приводятся в ЗБ. При определенных обстоятельствах, когда дополнительные

детализированные требования являются существенными и их реализация обязательна, необходимо в ЗБ повторно привести описание требований, приведенных в ПЗ;

г) если в ЗБ есть требование не только обеспечить соответствие ПЗ, но и расширить перечень задач и требований безопасности, то в разделах ЗБ, где имеются ссылки на ПЗ, должны быть приведены дополнительные задачи и требования безопасности. Если дополнительные задачи и требования безопасности являются существенными, то необходимо в ЗБ повторно привести описание задач и требований безопасности, приведенных в ПЗ.

В настоящем пособии не рассматриваются случаи, когда в ЗБ требуется лишь частичное его соответствие ПЗ.

В документе не устанавливается никаких правил описания в ЗБ задач и требований безопасности, приведенных в ПЗ, или ссылок на них. основополагающим является требование, чтобы содержание ЗБ было полным, ясным, исключало различные толкования, позволяло провести оценку ЗБ, являлось бы приемлемой основой для оценки объекта и допускало сравнение с любым нужным ПЗ.

Если имеется требование соответствия ЗБ нескольким ПЗ, то соответствующий раздел ЗБ должен для каждого ПЗ включать следующие данные:

1) ссылку на профиль защиты, на основе которой определяется тот ПЗ, которому должно соответствовать ЗБ, вместе со всеми дополнительными материалами, которые могут усилить условие соответствия. Правильно сформулированное условие соответствия (после усиления) подразумевает, что объект отвечает всем требованиям ПЗ;

2) уточнение профиля защиты, определяющее формулировки задач и требований безопасности объекта, которые удовлетворяют допустимым операциям ПЗ или проводят дальнейшую детализацию задач и требований безопасности, т.е. уточняют требования безопасности;

3) дополнение профиля защиты, определяющее формулировки задач и требований безопасности объекта, которые дополняют задачи и требования безопасности, приведенные в ПЗ.

### *Обоснование задания по безопасности*

Обоснование ЗБ должно подтвердить, что:

а) ЗБ содержит полную и взаимосвязанную совокупность требований безопасности;

б) разработанный в соответствии с заданными требованиями объект будет обладать эффективным набором средств обеспечения безопасности ИТ в среде безопасности;

в) общая спецификация объекта отражает заданные требования.

Обоснование также должно подтвердить соответствие ЗБ каждому ПЗ, указанному в ЗБ. В обоснование должны входить:

а) обоснование задач безопасности, которое подтверждает, что сформулированные задачи безопасности охватывают все указанные аспекты среды безопасности объекта и верно отражают их;

б) обоснование требований безопасности, которое подтверждает, что заданная совокупность требований безопасности объекта и его среды отвечает задачам безопасности.

При обосновании требований безопасности необходимо показать, что:

– совокупность компонентов функциональных и гарантийных требований объекта и его среды обеспечивает выполнение установленных задач безопасности объекта;

– набор требований безопасности образует единую и взаимосвязанную совокупность требований;

– выбор требований безопасности обоснован.

Специальное обоснование необходимо при задании требований, не содержащихся в СТБ 34.101.2 и СТБ 34.101.3, а также в случае неудовлетворенных зависимостей;

– выбор уровня стойкости СБ в ПЗ обоснован.

Требования к стойкости СБ должны быть согласованы с задачами безопасности объекта;

в) обоснование общей спецификации объекта, которое должно показывать, что СБ и гарантийные меры отвечают требованиям безопасности объекта.

При обосновании общей спецификации объекта необходимо показать, что:

– СБ реализуют функциональные требования безопасности объекта;

– требования к стойкости СБ обоснованы либо такие требования не предъявляются;

– подтверждено условие соответствия принятых мер гарантии гарантийным требованиям. Уровень детализации обоснования общей спецификации должен соответствовать уровню детализации описания КСБО;

г) обоснование требования соответствия профилям защиты, которое содержит объяснения различий между задачами и требованиями безопасности, представленными в ЗБ и в каждом ПЗ, соответствие которым должно быть обеспечено. Если в ЗБ отсутствует требование соответствия ПЗ или задачи и требования безопасности, представленные в ЗБ и в ПЗ, совпадают, то этот раздел в ЗБ можно опустить.

Обоснование должно предоставляться по желанию потребителей ЗБ.

### 3. МЕТОДОЛОГИЯ ОЦЕНКИ УРОВНЯ ЗАЩИЩЕННОСТИ ПРОДУКТОВ И СИСТЕМ ИНФОРМАЦИОННЫХ ТЕХНОЛОГИЙ

#### 3.1. Общая методология оценки

Процесс оценки состоит из выполнения оценщиком задачи получения исходных данных для оценки, подвидов деятельности по оценке и задачи оформления результатов оценки. На рис. 3.1 дается общее представление о взаимосвязи этих задач и подвидов деятельности по оценке.

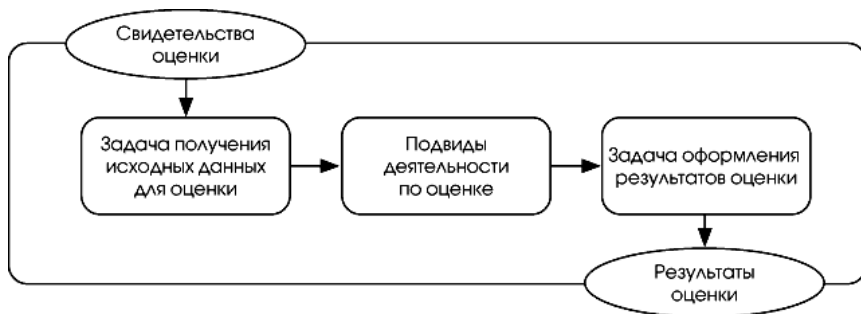


Рис. 3.1. Общая модель оценки

Подвиды деятельности по оценке варьируются в зависимости от того, оценивается ПЗ или ОО. Кроме того, при оценке ОО выбор подвидов деятельности зависит от специфицированных в ЗБ гарантийных требований (требований доверия). Между структурой «Общие критерии» (ОК) (класс – семейство – компонент – элемент) и

структурой «Общая методология оценки» (ОМО) (вид деятельности – подвид деятельности – действие – шаг оценивания) существует прямая взаимосвязь. На рис. 3.2 представлено соответствие между такими конструкциями ОК, как классы, компоненты и элементы действий оценщика, и рассматриваемыми в ОМО видами деятельности, подвидами деятельности и действиями. Вместе с тем, некоторые шаги оценивания ОМО могут прямо следовать из требований ОК, содержащихся в элементах действий разработчика, содержания и представления свидетельств.

*Примечание.*

1. «Общие критерии» как система взаимоувязанных метастандартов изложена в СТБ 34.101.1, СТБ 34.101.2, СТБ 34.101.3 и как производные от этих стандартов – в СТБ 34.101.6 и СТБ 34.101.7.

2. «Общая методология оценки» как система оценки (испытания) соответствия продуктов и систем ИТ (ИКТ) заданным уровням доверия (гарантии) изложена в СТБ 34.101.5.

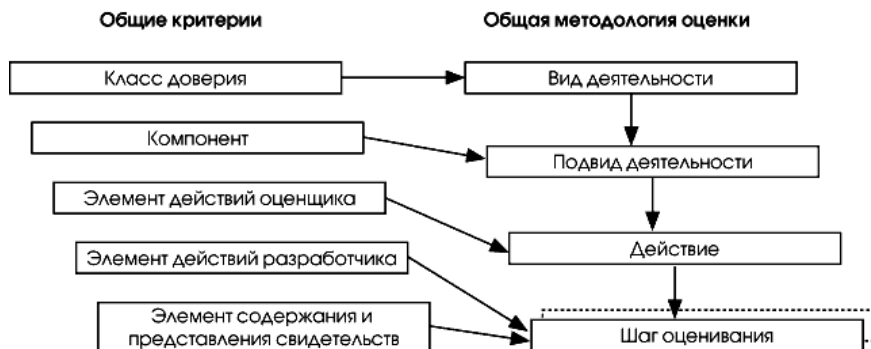


Рис. 3.2. Соотношение структур ОК и ОМО

В ОМО термин «Вид деятельности» (*activity*) используется для описания применения уровня гарантии (класса доверия) из части 3 ОК.

Для описания применения компонента доверия из части 3 ОК используется термин «Подвид деятельности» (*sub-activity*). Заметим, что семейства доверия прямо не рассматриваются в ОМО, поскольку при проведении оценки всегда используется только один компонент доверия из применяемого семейства. В свою очередь, с элементом действий оценщика из части 3 ОК связан термин «Действие» (*action*). Эти действия или сформулированы в явном виде как

действия оценщика, или неявно следуют из действий разработчика (подразумеваемые действия оценщика) в рамках компонентов доверия из части 3 ОК.

Термин «Шаг оценивания» (*work unit*) описывает неразделимый фрагмент работы по оценке. Каждое действие в ОМО включает один или несколько шагов оценивания, которые сгруппированы по элементам содержания и представления или действий разработчика соответствующего компонента из части 3 ОК. Шаги оценивания представлены в ОМО в том же порядке, что и элементы ОК, из которых они следуют. Шаги оценивания в соответствии с СТБ 34.101.5 содержат обязательные действия, которые оценщик должен выполнить, чтобы прийти к заключению о возможности отнесения продукта или системы ИКТ к тому или иному уровню гарантии (доверия) оценки.

*Примечание.* Данная методология применима для оценки продуктов и систем ИКТ, выполненных в защищенном исполнении.

## **3.2. Процесс оценки сервисов и механизмов информационной безопасности**

### **3.2.1. Особенности выполнения количественных оценок**

В настоящее время общеупотребительным подходом к построению критериев оценки безопасности ИТ является использование совокупности определенным образом упорядоченных качественных требований к функциональным механизмам обеспечения безопасности, их эффективности и доверия к реализации.

Качественные критерии применимы для оценки большей части механизмов обеспечения безопасности ИТ, а также оценки выполнения требований доверия к безопасности изделий ИТ. Несмотря на это, ОМО предусматривает возможность проведения там, где это применимо, количественных оценок с использованием соответствующих качественных показателей.

Чтобы корректно использовать количественный показатель, он должен иметь объективную интерпретацию, однозначную зависимость от отдельных аспектов безопасности. Поэтому количественные критерии целесообразно использовать для оценки таких механизмов безопасности, как парольная защита, контрольное суммирование и т.п.

### 3.2.2. Анализ стойкости функций безопасности как пример выполнения количественных оценок

В ОК и ОМО применение количественных показателей предусматривается при анализе стойкости функций безопасности (СФБ) ОО, реализованных вероятностными и/или перестановочными механизмами.

В процессе анализа оценщик определяет минимальный потенциал нападения, требуемый нарушителю, чтобы осуществить нападение, и приходит к заключению относительно возможностей ОО противостоять нападению. В табл. 3.1 демонстрируются и далее описываются взаимосвязи между анализом СФБ и потенциалом нападения.

Таблица 3.1

#### Стойкость функции безопасности и потенциал нападения

Уровень СФБ	Адекватная защита от нарушителя с потенциалом нападения	Недостаточная защита от нарушителя с потенциалом нападения
Высокая СФБ	высоким	не применимо – успешное нападение за пределами практически возможного
Средняя СФБ	умеренным	высоким
Базовая СФБ	низким	умеренным

Анализ стойкости функции безопасности ОО выполняется только для функций безопасности, реализуемых вероятностными или перестановочными механизмами, за исключением тех из них, которые основаны на криптографии. Более того, при анализе предполагается, что вероятностный или перестановочный механизм безопасности реализован безупречно и что функция безопасности используется при нападении с учетом ограничений ее проекта и реализации. Как показано в табл. 3.1, уровень СФБ также отражает нападение, описанное в терминах потенциала нападения, для защиты от которого спроектирована функция безопасности.

Потенциал нападения является функцией от мотивации, компетентности и ресурсов нарушителя.

При анализе стойкости функции безопасности предполагается наличие уязвимости в механизмах реализации этой функции безопасности ОО. Чтобы нарушитель мог использовать уязвимость, ему необ-

ходимо ее сначала идентифицировать, а затем только использовать. Это разделение может показаться тривиальным, но является существенным.

В ходе анализа потенциала нападения, требуемого для использования уязвимости, необходимо учитывать следующие факторы:

**1. При идентификации:**

1. время, затрачиваемое на идентификацию уязвимости;
2. техническую компетентность специалиста;
3. знание проекта и функционирования ОО;
4. доступ к ОО;
5. аппаратные средства/программное обеспечение ИТ или другое оборудование, требуемое для анализа.

**2. При использовании:**

- 1) время, затрачиваемое на использование уязвимости;
- 2) техническую компетентность специалиста;
- 3) знание проекта и функционирования ОО;
- 4) доступ к ОО;
- 5) аппаратные средства/программное обеспечение ИТ или другое оборудование, требуемое для использования уязвимости.

Фактор **«Время»** – это время, обычно затрачиваемое нарушителем на непрерывной основе, чтобы идентифицировать или использовать уязвимость. Данный фактор может иметь следующие значения: «за минуты» (при нападении идентификация и использование уязвимости занимает менее получаса); «за часы» (менее чем за день); «за дни» (менее, чем за месяц) и «за месяцы» (нападение требует, по меньшей мере, месяца).

Фактор **«Компетентность специалиста»** относится к уровню общих знаний прикладной области или типа продукта (например, операционной системы, протоколов Интернета). Идентифицированными уровнями компетентности являются следующие:

1. **«Эксперты»** хорошо знакомы с основными алгоритмами, протоколами, аппаратными средствами, структурами и т.п., реализованными в типе продукта или системы, а также с применяемыми принципами и концепциями безопасности.

2. **«Профессионалы»** хорошо осведомлены в том, что касается режима безопасности продукта или системы данного типа.



3. **«Непрофессионалы»** слабо осведомлены, по сравнению с экспертами или профессионалами, и не обладают специфической компетентностью.

Фактор **«Знание ОО»** указывает на определенный уровень знаний об ОО. Оно отличается от общей компетентности, хотя и связано с ней. Идентифицированными уровнями знания ОО являются следующие:

1. **«Отсутствие информации»** об ОО, кроме его назначения.

2. **«Общедоступная информация»** об ОО (например, полученная из руководства пользователя).

3. **«Чувствительная информация»** об ОО (например, сведения о внутреннем содержании проекта).

**«Доступ к ОО»** также является важным фактором и имеет отношение к фактору **«Время»**. Идентификация или использование уязвимости могут требовать продолжительного доступа к ОО, что может увеличить вероятность обнаружения. Некоторые нападения могут требовать значительных автономных усилий и лишь краткого доступа к ОО для использования уязвимости. Также может быть необходим доступ непрерывный или в виде нескольких сеансов.

Фактор **«Аппаратные средства/программное обеспечение ИТ или другое оборудование»** указывает на оборудование, которое требуется для идентификации или использования уязвимости.

В качестве значений данного фактора рассматриваются следующие виды оборудования:

1) **стандартное оборудование** – это оборудование либо для идентификации уязвимости, либо для нападения, которое легко доступно нарушителю. Это оборудование может быть частью самого ОО (например, отладчик в операционной системе) или может быть легко получено (например, программное обеспечение, загружаемое из Интернета);

2) **специализированное оборудование** не является общедоступным, но может быть приобретено нарушителем без значительных усилий. Оно может включать покупку небольшого количества оборудования (например, анализатора протоколов) или разработку более сложных сценариев и программ нападения;

3) **заказное оборудование** – это оборудование, которое либо может потребовать его специальной разработки (например, очень сложное программное обеспечение), либо настолько специализирован-

ное, что его распространение контролируется и, возможно, даже ограничено, либо является очень дорогим. Использование сотен персональных компьютеров, связанных через Интернет, как правило, относится к этой категории.

В табл. 3.2 значениям (диапазонам значений) рассмотренных факторов поставлены в соответствие числовые значения по двум аспектам: идентификации уязвимости и использованию уязвимости.

Таблица 3.2

Вычисление потенциала нападения

Название фактора	Диапазон	Значение при идентификации уязвимости	Значение при использовании уязвимости
Заграниваемое время	< 0,5 часа	0	0
	< 1 дня	2	3
	< 1 месяца	3	5
	> 1 месяца	5	8
	Не практически	*	*
Компетентность	Непрофессионал	0	0
	Профессионал	2	2
	Эксперт	5	4
Знание ОО	Отсутствие информации	0	0
	Общедоступная информация	2	2
	Чувствительная информация	5	4
Доступ к ОО	< 0,5 часа или не обнаруживаемый доступ	0	0
	< 1 дня	2	4
	< 1 месяца	3	6
	> 1 месяца	4	9
	Не практически	*	*
Оборудование	Отсутствует	0	0
	Стандартное	1	2
	Специализированное	3	4
	Заказное	5	6

\* Означает, что нападение невозможно в пределах тех временных рамок, которые были бы приемлемы для нарушителя. Любое значение «\*» указывает на противостояние нарушителю с высоким потенциалом нападения.

При определении потенциала нападения для данной уязвимости из каждого столбца (столбцы 3 и 4 табл. 3.2) для каждого фактора следует выбрать определенное значение (10 значений). При выборе значений должна учитываться предопределенная среда ОО. Выбранные 10 значений суммируются, давая итоговое значение. Это значение затем сверяется с табл. 3.3 для определения рейтинга уязвимости и соответственно по табл. 3.1 – уровня СФБ. Полученный уровень стойкости функции безопасности говорит о том, нарушителю с каким потенциалом противостоит ОО.

Таблица 3.3

#### Рейтинг уязвимостей

Диапазон значений	ОО противостоит нарушителю с потенциалом нападения
< 10	нет рейтинга
10–17	низким
18–24	умеренным
> 25	высоким

Когда значение фактора оказывается близким к границе диапазона, то оценщику следует подумать об использовании значения, усредняющего табличные данные. Например, если для использования уязвимости требуется доступ к ОО в течение одного часа или если доступ обнаруживается очень быстро, то для этого фактора может быть выбрано значение между 0 и 4.

Для конкретной уязвимости может возникнуть необходимость сделать несколько проходов (см. табл. 3.2) для различных сценариев нападения (например, попеременно использовать разные значения компетентности в сочетании с определенными значениями факторов времени или оборудования). При этом ориентироваться нужно на наименьшее значение, полученное для этих проходов.

В случае уязвимости, которая уже идентифицирована и информация о которой общедоступна, «**при идентификации уязвимости**»

нарушителем (столбец 3 табл. 3.2) значения следует выбирать, исходя из раскрытия этой уязвимости в общедоступных источниках, а не из начальной ее идентификации нарушителем.

### 3.2.3. Пример анализа стойкости функции безопасности

Рассмотрим пример анализа СФБ для гипотетического механизма цифрового пароля.

Информация, полученная из ЗБ и свидетельств проекта, показывает, что идентификация и аутентификация предоставляют основу для управления доступом к сетевым ресурсам с терминалов, расположенных далеко друг от друга. Управление физическим доступом к терминалам и контроль продолжительности сеанса каким-либо эффективным способом не осуществляется. Уполномоченные пользователи системы подбирают себе свои собственные цифровые пароли для входа в систему во время начальной авторизации использования системы и в дальнейшем – по запросу пользователя. Система содержит ограничения на цифровые пароли, выбираемые пользователем. Эти исходные данные получены на основе анализа функциональных требований безопасности из ЗБ (рис. 3.3).

Предполагается, что пароли состоят не менее чем из четырех символов, являющихся цифрами. Все цифры должны быть различны. Кроме того, запрещается использовать «явно неслучайные» пароли, представляющие собой последовательно возрастающие или убывающие совокупности цифр (1234, 8765 и т.п.) или связанные каким-либо способом с конкретным пользователем, например, с датой рождения.

Число возможных значений цифровых паролей рассчитывается способом, приведенным далее.

Если допустить самый плохой вариант сценария, когда пользователь выбирает число, состоящее только из четырех цифр, то число перестановок цифрового пароля (предполагается, что каждая цифра уникальна) равно  $7 \times 8 \times 9 \times 10 = 5040$ .

Число возможных увеличивающихся рядов – семь, как и число убывающих рядов. После отбрасывания этих рядов число возможных значений цифровых паролей равно  $5040 - 14 = 5026$ .

Основываясь на дополнительной информации (см. рис. 3.3) в механизме цифрового пароля спроектирована характеристика блокировки терминала. После шестой подряд неудачной попытки аутентификации терминал блокируется на один час. Счетчик неудачной

аутентификации сбрасывается через пять минут; таким образом, нарушитель в лучшем случае может осуществить пять попыток ввода цифрового пароля каждые пять минут или 60 вводов цифрового пароля в час.

<b>1. Ограничения на цифровые пароли:</b>	
<b>FIA_SOS.1</b>	<b>Верификация секретов</b>
FIA_SOS.1.1	ФБО должны предоставить механизм для верификации того, что <b>пароли</b> отвечают следующей метрике качества: <ul style="list-style-type: none"><li>– цифровой пароль должен быть не менее четырех и не более шести цифр;</li><li>– последовательные числовые ряды типа (7, 6, 5, 4, 3, 2, 1) не допускаются;</li><li>– повторение цифр не допускается (каждая цифра должна быть уникальной).</li></ul>
<b>2. Характеристики блокировки терминала:</b>	
<b>FIA_AFL.1(1)</b>	<b>Обработка отказов аутентификации</b>
FIA_AFL.1.1	ФБО должна обнаруживать, когда произойдет (очередная) неуспешная попытка аутентификации (для данного терминала с момента последней попытки аутентификации или сброса счетчика неудачной аутентификации).
FIA_AFL.1.2	При <b>обнаружении</b> неуспешной попытки аутентификации ФБО должны увеличить значение счетчика неудачной аутентификации на единицу. При этом сброс (обнуление) счетчика осуществляется через пять минут.
<b>FIA_AFL.1(2)</b>	<b>Обработка отказов аутентификации</b>
FIA_AFL.1.1	ФБО должна обнаруживать, когда произойдет шесть неуспешных попыток аутентификации (для данного терминала с момента последней попытки или с момента последнего сброса счетчика неудачной аутентификации).
FIA_AFL.1.2	При достижении счетчиком <b>неуспешных попыток аутентификации</b> , определенного в элементе <b>FIA_AFL.1.1</b> , <b>ФБО</b> должны выполнить блокирование терминала на один час.

Рис. 3.3. Функциональные требования безопасности как источник для расчета стойкости функции безопасности

В среднем, нарушитель должен был бы ввести 2513 цифровых комбинаций до ввода правильного цифрового пароля. Как резуль-

тат, в среднем, успешное нападение произошло бы чуть меньше, чем за 2513 мин / (60 мин/ч) ~ 42 ч.

Значения факторов при идентификации следует выбирать минимальными из каждой категории (все 0), так как существование уязвимости в рассматриваемой функции очевидно.

Основываясь на приведенных выше вычислениях, можно судить о том, что для непрофессионала является возможным нанести поражение механизму в пределах дней (при получении доступа к ОО) без использования какого-либо оборудования и без знания ОО, что в соответствии с табл. 3.3, (для использования уязвимостей) дает значение 11. Получив результирующую сумму 11, потенциал нападения, требуемый для осуществления успешной атаки, можно опделить по меньшей мере как низкий.

Поскольку механизм цифрового пароля является стойким к нарушителю с низким потенциалом, то этот механизм цифрового пароля соответствует уровню «базовая СФБ» (см. табл. 3.1).

#### **4. ВЫПОЛНЕНИЕ ПРОЕКТА В ЭЛЕКТРОННОЙ ФОРМЕ**

По решению кафедры может быть разрешено представление проекта в электронной форме. При этом студент выполняет весь объем работ. Изменяется только перечень и форма представляемых к защите материалов.

К защите студент представляет пояснительную записку в печатном виде, в которую входят:

- а) титульный лист;
- б) лист задания;
- в) реферат;
- г) выводы;
- д) опись файлов проекта, находящихся на электронных носителях – дискетах 3,5", компакт диске (только CD-R, не CD-RW).

Основные материалы работы представляются на электронных носителях информации в следующем виде:

- в файле index – опись файлов проекта (работы);
- в каталоге DOC – пояснительная записка и графические материалы;

– в каталоге EXE – исполняемые файлы и файлы разработанных приложений;

– в каталоге GRAF – иллюстративный материал и файлы презентации.

Структура пояснительной записки должна поддерживать форматирование стилями и обеспечивать формирование оглавления в автоматическом режиме. Наименования в тексте (подписи к рисункам и таблицам) должны иметь уникальные обозначения, формирование которых должно производиться в автоматическом режиме. Все главы и разделы пояснительной записки должны иметь единое стилистическое оформление.

Опись файлов проекта (работы) оформляется в соответствии с таблицей и представляется отдельным файлом **index** в формате **rtf**. Файл описи размещается на первом носителе. Имена файлов должны отражать индивидуальные особенности проекта: номер группы (последние три цифры), фамилию студента (сокращается до трех–пяти букв) или название темы проекта.

## НОРМАТИВНЫЕ ДОКУМЕНТЫ

1. СТБ 34.101.1–2004 (ИСО/МЭК 15408-1:1999) «Информационные технологии и безопасность. Критерии оценки безопасности информационных технологий. Часть 1. Введение и общая модель».

2. СТБ 34.101.2–2004 (ИСО/МЭК 15408-2:1999) «Информационные технологии и безопасность. Критерии оценки безопасности информационных технологий. Часть 2. Функциональные требования безопасности».

3. СТБ 34.101.3–2004 (ИСО/МЭК 15408-3:1999) «Информационные технологии и безопасность. Критерии оценки безопасности информационных технологий. Часть 3. Гарантийные требования безопасности».

4. СТБ 34.101.4–2004 «Информационные технологии. Методы и средства безопасности. Профиль защиты электронной почты предприятия».

5. СТБ П 34.101.5–2003 «Информационные технологии и безопасность. Общая методология испытаний продуктов и систем информационных технологий на соответствие уровням гарантий».

6. СТБ П 34.101.6–2003 «Информационные технологии и безопасность. Задание по обеспечению безопасности. Разработка, обоснование, оценка».

7. СТБ 34.101.7–2003 «Информационные технологии и безопасность. Профиль защиты. Разработка, обоснование, оценка».

8. СТБ П 34.101.8–2003 «Информационные технологии. Методы и средства безопасности. Программные средства защиты от воздействия вредоносных программ и антивирусные программные средства. Общие требования».

9. СТБ 34.101.9–2004 «Информационные технологии. Требования к защите информации от несанкционированного доступа, устанавливаемые в техническом задании на создание автоматизированной системы».

10. СТБ 34.101.10–2004 «Информационные технологии. Средства защиты информации от несанкционированного доступа в автоматизированных системах. Общие требования».

11. СТБ 34.101.11–2004 «Информационные технологии. Методы и средства безопасности. Критерии оценки безопасности информационных технологий. Профиль защиты операционной системы сервера для использования в доверенной зоне корпоративной сети».

12. СТБ 34.101.12–2004 «Информационные технологии. Методы и средства безопасности. Программные средства защиты от воздействия вредоносных программ и антивирусные программные средства. Оценка качества».

13. СТБ 34.101.13–2004 «Информационные технологии. Методы и средства безопасности. Критерии оценки безопасности информационных технологий. Профиль защиты операционной системы сервера для использования в демилитаризованной зоне корпоративной сети».

14. СТБ П 34.101.14–2004 «Информационные технологии. Методы и средства безопасности. Критерии оценки безопасности информационных технологий. Профиль защиты программных средств маршрутизатора для использования в демилитаризованной зоне корпоративной сети».

15. СТБ П 34.101.15–2004 «Информационные технологии. Методы и средства безопасности. Программные средства защиты от воздействия вредоносных программ и антивирусные программные средства. Типовая программа и методика испытаний».



16. СТБ П 34.101.16–2004 «Информационные технологии. Методы и средства безопасности. Критерии оценки безопасности информационных технологий. Профиль защиты программных средств коммутатора для использования в доверенной зоне корпоративной сети».

17. СТБ 1176.1–99 «Информационная технология. Криптографическая защита информации. Функция хэширования».

18. СТБ 1176.2–99 «Информационная технология. Криптографическая защита информации. Процедуры выработки и проверка электронной цифровой подписи».

19. ГОСТ 28147–89 «Системы обработки информации. Защита криптографическая. Алгоритм криптографических преобразований».

20. СТБ ИСО/МЭК 17799:2005 «Управление информационной безопасностью».

21. СТБ ГОСТ Р 51318.24–2001 «Совместимость технических средств электромагнитная. Устойчивость оборудования информационных технологий к электромагнитным помехам. Требования и методы испытаний».

22. СТБ П 34.101.31–2007 «Информационные технологии. Методы и средства безопасности. Криптографические алгоритмы шифрования и контроля целостности».

23. Common Evaluation Methodology for Information Technology Security Evaluation. Part 1: Introduction and general model, version 0.6, 19 January 1997.

24. Common Evaluation Methodology for Information Technology Security Evaluation. Part 2: Evaluation Methodology, version 1.0, August 1999.

25. РД «Безопасность информационных технологий. Общая методология оценки безопасности информационных технологий». – Гостехкомиссия России, 2004.

26. РД «Безопасность информационных технологий. Типовая методика оценки безопасности профилей защиты и заданий по безопасности». – Гостехкомиссия России, 2004.

Учебное издание

АРТАМОНОВ Владимир Афанасьевич

ПРОЕКТИРОВАНИЕ СИСТЕМ ЗАЩИТЫ  
КОМПЬЮТЕРНОЙ ИНФОРМАЦИИ

Методическое пособие  
по курсовому проектированию

Редактор Т.А. Подолякова  
Компьютерная верстка Н.А. Школьниковой

---

Подписано в печать 21.02.2011.

Формат 60×84<sup>1</sup>/<sub>16</sub>. Бумага офсетная.

Отпечатано на ризографе. Гарнитура Таймс.

Усл. печ. л. 3,78. Уч.-изд. л. 2,95. Тираж 200. Заказ 701.

---

Издатель и полиграфическое исполнение:  
Белорусский национальный технический университет.  
ЛИ № 02330/0494349 от 16.03.2009.  
Проспект Независимости, 65. 220013, Минск.