

МИНИСТЕРСТВО НАУКИ И ВЫСШЕГО ОБРАЗОВАНИЯ РОССИЙСКОЙ ФЕДЕРАЦИИ

**ПОЛИТЕХНИЧЕСКИЙ ИНСТИТУТ (ФИЛИАЛ)**

**ФЕДЕРАЛЬНОГО ГОСУДАРСТВЕННОГО БЮДЖЕТНОГО**

**ОБРАЗОВАТЕЛЬНОГО УЧРЕЖДЕНИЯ ВЫСШЕГО ОБРАЗОВАНИЯ**

**«ДОНСКОЙ ГОСУДАРСТВЕННЫЙ ТЕХНИЧЕСКИЙ УНИВЕРСИТЕТ»**

**В Г. ТАГАНРОГЕ РОСТОВСКОЙ ОБЛАСТИ**

**ПИ (филиал) ДГТУ в г. Таганроге**

УТВЕРЖДАЮ

Директор

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ А.К. Исаев

«\_\_\_»\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_2019 г

Рег. № \_\_\_\_\_\_\_\_\_\_\_\_

**УЧЕБНО-МЕТОДИЧЕСКОЕ ПОСОБИЕ**

к практическим занятиям

по учебной дисциплине ОП.09 Стандартизация, сертификация и техническое

по специальности 09.02.07 «Информационные системы и программирование»

Таганрог

2020

**Лист согласования**

Учебно-методическое пособие по учебные дисциплиныСтандартизация, сертификация и техническое документоведение разработана на основе Федерального государственного образовательного стандарта (далее – ФГОС) для специальности среднего профессионального образования (далее – СПО) 09.02.07 «Информационные системы и программирование».

**Разработчик(и):**

Преподаватель \_\_\_\_\_\_\_\_\_\_\_\_\_ Т.М. Марданова

Методические указания рассмотрены и одобрены на заседании цикловой методической комиссии специальности 09.02.05Прикладная информатика (по отраслям)

Протокол № 7 от «04» февраля 2020г

Председатель цикловой методической комиссии О.В. Андриян

**Рецензенты:**

ЧОУ ВО «ТИУиЭ» начальник информационно-аналитического управления, к.т.н., доцент О.И. Овчаренко

АО «Красный гидропресс»зам. начальника отдела ИТ С.С. Пирожков

**Согласовано:**

Заведующий УМО

Т. В. Воловская

**ВВЕДЕНИЕ**

В учебно-методическом пособии к практикуму по курсу «Стандартизация, сертификация и техническое документоведение» изложены сведения, необходимые для успешного выполнения практических занятий по данному курсу. Описан процесс работы с инструментарием, применяемым на практических занятиях, представлен ряд типичных задач и подходы к их решению. В целях глубокого усвоения студентами изучаемого матери­ала по дисциплине «Стандартизация, сертификация и техническое документоведение» в комплексе с изло­жением теоретических вопросов, также Применять требования нормативных актов к основным видам продукции (услуг) и процессов. Применять документацию систем качества.

Цель настоящего пособия полученние студентами навыки правового анализа юридических норм и принятия грамотных процессуальных решений в практической деятельности.

Обучающийся должен знать: Правовые основы метрологии, стандартизации и сертификации. Основные понятия и определения метрологии, стандартизации и сертификации. Основные положения систем (комплексов) общетехнических и организационно-методических стандартов. Показатели качества и методы их оценки. Системы качества. Основные термины и определения в области сертификации. Организационную структуру сертификации. Системы и схемы сертификации.

Обучающийся должен уметь: Применять требования нормативных актов к основным видам продукции (услуг) и процессов. Применять документацию систем качества. Применять основные правила и документы системы сертификации Российской Федерации.

**Правила выполнения практических занятий**

Практические занятия выполняются каждым обучающимся самостоятельно в полном объеме и согласно содержанию методических указаний.

Перед выполнением обучающийся должен отчитаться перед преподавателем за выполнение предыдущего занятия (сдать отчет).

Обучающийся должен на уровне понимания и воспроизведения предварительно усвоить необходимую для выполнения практических занятий теоретическую и информацию.

Обучающийся, получивший положительную оценку и сдавший отчет по предыдущему практическому занятию, допускается к выполнению следующему занятию.

Обучающийся, пропустивший практическое занятие по уважительной либо неуважительной причине, закрывает задолженность в процессе выполнения последующих практических занятий.

**Практическая работа №1. Нормативно-правовые документы и стандарты в области защиты информации и информационной безопасности. Системы менеджмента качества**

Цель работы:

Изучить законодательный уровень информационной безопасности.

**1. Теоретическое введение**

**1.1. Что такое законодательный уровень информационной безопасности ?**

В деле обеспечения информационной безопасности успех может принести только комплексный подход. Мы уже указывали, что для защиты интересов субъектов информационных отношений необходимо сочетать меры следующих уровней:

* законодательного;
* административного (приказы и другие действия руководства организаций, связанных с защищаемыми информационными системами);
* процедурного (меры безопасности, ориентированные на людей);
* программно-технического.

Законодательный уровень является важнейшим для обеспечения информационной безопасности. Большинство людей не совершают противоправных действий не потому, что это технически невозможно, а потому, что это осуждается и/или наказывается обществом, потому, что так поступать не принято.

Мы будем различать на законодательном уровне две группы мер:

* меры, направленные на создание и поддержание в обществе негативного (в том числе с применением наказаний) отношения к нарушениям и нарушителям информационной безопасности (назовем их мерами ограничительной направленности);
* направляющие и координирующие меры, способствующие повышению образованности общества в области информационной безопасности, помогающие в разработке и распространении средств обеспечения информационной безопасности (меры созидательной направленности).

На практике обе группы мер важны в равной степени, но нам хотелось бы выделить аспект осознанного соблюдения норм и правил ИБ. Это важно для всех субъектов информационных отношений, поскольку рассчитывать только на защиту силами правоохранительных органов было бы наивно. Необходимо это и тем, в чьи обязанности входит наказывать нарушителей, поскольку обеспечить доказательность при расследовании и судебном разбирательстве компьютерных преступлений без специальной подготовки невозможно.

Самое важное (и, вероятно, самое трудное) на законодательном уровне - создать механизм, позволяющий согласовать процесс разработки законов с реалиями и прогрессом информационных технологий. Законы не могут опережать жизнь, но важно, чтобы отставание не было слишком большим, так как на практике, помимо прочих отрицательных моментов, это ведет к снижению информационной безопасности.

**1.2. Обзор российского законодательства в области информационной безопасности**

**1.2.1. Правовые акты общего назначения, затрагивающие вопросы информационной безопасности**

Основным законом Российской Федерации является Конституция, принятая 12 декабря 1993 года.

В соответствии со статьей 24 Конституции, органы государственной власти и органы местного самоуправления, их должностные лица обязаны обеспечить каждому возможность ознакомления с документами и материалами, непосредственно затрагивающими его права и свободы, если иное не предусмотрено законом.

Статья 41 гарантирует право на знание фактов и обстоятельств, создающих угрозу для жизни и здоровья людей, статья 42 - право на знание достоверной информации о состоянии окружающей среды.

В принципе, право на информацию может реализовываться средствами бумажных технологий, но в современных условиях наиболее практичным и удобным для граждан является создание соответствующими законодательными, исполнительными и судебными органами информационных серверов и поддержание доступности и целостности представленных на них сведений, то есть обеспечение их (серверов) информационной безопасности.

Статья 23 Конституции гарантирует право на личную и семейную тайну, на тайну переписки, телефонных переговоров, почтовых, телеграфных и иных сообщений, статья 29 - право свободно искать, получать, передавать, производить и распространять информацию любым законным способом. Современная интерпретация этих положений включает обеспечение конфиденциальности данных, в том числе в процессе их передачи по компьютерным сетям, а также доступ к средствам защиты информации.

В Гражданском кодексе Российской Федерации (в своем изложении мы опираемся на редакцию от 15 мая 2001 года) фигурируют такие понятия, как банковская, коммерческая и служебная тайна. Согласно статье 139, информация составляет служебную или коммерческую тайну в случае, когда информация имеет действительную или потенциальную коммерческую ценность в силу неизвестности ее третьим лицам, к ней нет свободного доступа на законном основании, и обладатель информации принимает меры к охране ее конфиденциальности. Это подразумевает, как минимум, компетентность в вопросах ИБ и наличие доступных (и законных) средств обеспечения конфиденциальности.

Весьма продвинутым в плане информационной безопасности является Уголовный кодекс Российской Федерации (редакция от 14 марта 2002 года). Глава 28 - "Преступления в сфере компьютерной информации" - содержит три статьи:

* статья 272. Неправомерный доступ к компьютерной информации;
* статья 273. Создание, использование и распространение вредоносных программ для ЭВМ;
* статья 274. Нарушение правил эксплуатации ЭВМ, системы ЭВМ или их сети.

Первая имеет дело с посягательствами на конфиденциальность, вторая - с вредоносным ПО, третья - с нарушениями доступности и целостности, повлекшими за собой уничтожение, блокирование или модификацию охраняемой законом информации ЭВМ. Включение в сферу действия УК РФ вопросов доступности информационных сервисов представляется нам очень своевременным.

Статья 138 УК РФ, защищая конфиденциальность персональных данных, предусматривает наказание за нарушение тайны переписки, телефонных переговоров, почтовых, телеграфных или иных сообщений. Аналогичную роль для банковской и коммерческой тайны играет статья 183 УК РФ.

Интересы государства в плане обеспечения конфиденциальности информации нашли наиболее полное выражение в Законе "О государственной тайне"(с изменениями и дополнениями от 6 октября 1997 года). В нем гостайна определена как защищаемые государством сведения в области его военной, внешнеполитической, экономической, разведывательной, контрразведывательной и оперативно-розыскной деятельности, распространение которых может нанести ущерб безопасности Российской Федерации. Там же дается определение средств защиты информации. Согласно данному Закону, это технические, криптографические, программные и другие средства, предназначенные для защиты сведений, составляющих государственную тайну.

Первая имеет дело с посягательствами на конфиденциальность, вторая - с вредоносным ПО, третья - с нарушениями доступности и целостности, повлекшими за собой уничтожение, блокирование или модификацию охраняемой законом информации ЭВМ. Включение в сферу действия УК РФ вопросов доступности информационных сервисов представляется нам очень своевременным.

Статья 138 УК РФ, защищая конфиденциальность персональных данных, предусматривает наказание за нарушение тайны переписки, телефонных переговоров, почтовых, телеграфных или иных сообщений. Аналогичную роль для банковской и коммерческой тайны играет статья 183 УК РФ.

Интересы государства в плане обеспечения конфиденциальности информации нашли наиболее полное выражение в Законе "О государственной тайне**"**(с изменениями и дополнениями от 6 октября 1997 года). В нем гостайна определена как защищаемые государством сведения в области его военной, внешнеполитической, экономической, разведывательной, контрразведывательной и оперативно-розыскной деятельности, распространение которых может нанести ущерб безопасности Российской Федерации. Там же дается определение средств защиты информации. Согласно данному Закону, это технические, криптографические, программные и другие средства, предназначенные для защиты сведений, составляющих государственную тайну; средства, в которых они реализованы, а также средства контроля эффективности защиты информации. Подчеркнем важность последней части определения.

**Порядок выполнения работы**

1.Ознакомиться с российским зарубежным законодательством в области ИБ..

2.Выполнить практическое задание.

3.Ответить на контрольные вопросы.

**3. Практические задания**

**1. Разработать интерфейс пользователя «Обзор российского законодательства в области информационной безопасности».**

**2. Разработать интерфейс пользователя «Обзор зарубежного законодательства в области информационной безопасности».**

**4. Контрольные вопросы**

**Вариант 1**

**1. Уголовный кодекс РФ не предусматривает наказания за:**

* неправомерный доступ к компьютерной информации
* создание, использование и распространение вредоносных программ
* массовую рассылку незапрошенной рекламной информации.

**2. Согласно Закону "Об информации, информатизации и защите информации", персональные данные — это:**

* сведения о фактах, событиях и обстоятельствах жизни гражданина, позволяющие идентифицировать его личность
* данные, хранящиеся в персональном компьютере
* данные, находящиеся в чьей-либо персональной собственности

**3. Согласно Закону "О лицензировании отдельных видов деятельности", лицензия — это:**

* специальное разрешение на осуществление конкретного вида деятельности
* удостоверение, подтверждающее высокое качество изделия
* документ, гарантирующий безопасность программного продукта

**4. В законопроекте "О совершенствовании информационной безопасности" (США, 2001 год) особое внимание обращено на:**

* системы электронной коммерции
* инфраструктуру для электронных цифровых подписей
* средства электронной аутентификации

**Вариант 2**

**1. Уголовный кодекс РФ не предусматривает наказания за:**

* увлечение компьютерными играми в рабочее время
* неправомерный доступ к компьютерной информации
* нарушение правил эксплуатации ЭВМ, системы ЭВМ или их сети

**2. Согласно Закону "Об информации, информатизации и
защите информации", конфиденциальная информация —
это:**

* информация с грифом "секретно"
* документированная информация, доступ к которой ограничивается в соответствии с законодательством Российской Федерации
* информация, доступ к которой ограничивается сертифицированными техническими средствами

**3. Действие Закона "О лицензировании отдельных видов
деятельности" не распространяется на:**

* деятельность по технической защите конфиденциальной информации
* образовательную деятельность в области защиты информации
* предоставление услуг в области шифрования информации

**4. В следующих странах сохранилось жесткое
государственное регулирование разработки и
распространения криптосредств на внутреннем рынке:**

* Китай
* Россия
* Франция

**Вариант 3**

**1. Уголовный кодекс РФ не предусматривает наказания за:**

* создание, использование и распространение вредоносных программ
* ведение личной корреспонденции на производственной технической базе
* нарушение правил эксплуатации ЭВМ, системы ЭВМ или их сети

**2. Согласно Закону "Об информации, информатизации и
защите информации", риск, связанный с использованием
информации, полученной из несертифицированной системы, лежит на:**

* + владельце этой системы
	+ собственнике документов
	+ потребителе информации

**3. Действие Закона "О лицензировании отдельных видов
деятельности" распространяется на:**

* деятельность по использованию шифровальных (криптографических) средств
* деятельность по рекламированию шифровальных (криптографических) средств
* деятельность по распространению шифровальных (криптографических) средств

**4. В законопроекте "О совершенствовании информационной
безопасности" (США, 2001 год) особое внимание
обращено на:**

* + смягчение ограничений на экспорт криптосредств
	+ разработку средств электронной аутентификации
	+ создание инфраструктуры с открытыми ключами

**Практическая работа №2**. Стандарты и спецификации в области информационной безопасности.

# Цель работы:

Изучить международные и национальные стандарты и спецификации в области ИБ — от "Оранжевой книги" до ISO 15408. Получить навыки определения сильных и слабых стороны этих документов.

.**1. Теоретическое введение**

#### Оценочные стандарты и технические спецификации.

#### «Оранжевая книга» как оценочный стандарт»

#### 1.1.1. Основные понятия

Мы приступаем к обзору стандартов и спецификаций двух разных видов:

* оценочных стандартов, направленных на классификацию информационных систем и средств защиты по требованиям безопасности;
* технических спецификаций, регламентирующих различные аспекты реализации средств защиты.

Важно отметить, что между эти видами нормативных документов нет глухой стены. Оценочные стандарты выделяют важнейшие, с точки зрения ИБ, аспекты ИС, играя роль архитектурных спецификаций. Другие технические спецификации определяют, как строить ИС предписанной архитектуры.

Исторически первым оценочным стандартом, получившим широкое распространение и оказавшим огромное влияние на базу стандартизации ИБ во многих странах, стал стандарт Министерства обороны США "Критерии оценки доверенных компьютерных систем".

Данный труд, называемый чаще всего по цвету обложки "Оранжевой книгой", был впервые опубликован в августе 1983 года. Уже одно его название требует комментария. Речь идет не о безопасных, а о доверенных системах, то есть системах, которым можно оказать определенную степень доверия.

"Оранжевая книга" поясняет понятие безопасной системы, которая "управляет, с помощью соответствующих средств, доступом к информации, так что только должным образом авторизованные лица или процессы, действующие от их имени, получают право читать, записывать, создавать и удалять информацию".

Очевидно, однако, что абсолютно безопасных систем не существует, это абстракция. Есть смысл оценивать лишь степень доверия, которое можно оказать той или иной системе.

В "Оранжевой книге" доверенная система определяется как "система, использующая достаточные аппаратные и программные средства, чтобы обеспечить одновременную обработку информации разной степени секретности группой пользователей без нарушения прав доступа".

Обратим внимание, что в рассматриваемых Критериях и безопасность, и доверие оцениваются исключительно с точки зрения управления доступом к данным, что является одним из средств обеспечения конфиденциальности и целостности (статической). Вопросы доступности "Оранжевая книга" не затрагивает.

Степень доверия оценивается по двум основным критериям.

1. **Политика безопасности** - набор законов, правил и норм поведения, определяющих, как организация обрабатывает, защищает и распространяет информацию. В частности, правила определяют, в каких случаях пользователь может оперировать конкретными наборами данных. Чем выше степень доверия системе, тем строже и многообразнее должна быть политика безопасности. В зависимости от сформулированной политики можно выбирать конкретные механизмы обеспечения безопасности. Политика безопасности - это активный аспект защиты, включающий в себя анализ возможных угроз и выбор мер противодействия.
2. **Уровень гарантированности** - мера доверия, которая может быть оказана архитектуре и реализации ИС. Доверие безопасности может проистекать как из анализа результатов тестирования, так и из проверки (формальной или нет) общего замысла и реализации системы в целом и отдельных ее компонентов. Уровень гарантированности показывает, насколько корректны механизмы, отвечающие за реализацию политики безопасности. Это пассивный аспект защиты.

Важным средством обеспечения безопасности является механизм **подотчетности**(протоколирования). Доверенная система должна фиксировать все события, касающиеся безопасности. Ведение протоколов должно дополняться аудитом, то есть анализом регистрационной информации.

Концепция доверенной вычислительной базы является центральной при оценке степени доверия безопасности. Доверенная вычислительная база - это совокупность защитных механизмов ИС (включая аппаратное и программное обеспечение), отвечающих за проведение в жизнь политики безопасности. Качество вычислительной базы определяется исключительно ее реализацией и корректностью исходных данных, которые вводит системный администратор.

Вообще говоря, компоненты вне вычислительной базы могут не быть доверенными, однако это не должно влиять на безопасность системы в целом. В результате, для оценки доверия безопасности ИС достаточно рассмотреть только ее вычислительную базу, которая, как можно надеяться, достаточно компактна.

Основное назначение доверенной вычислительной базы - выполнять функции монитора обращений, то есть контролировать допустимость выполнения субъектами (активными сущностями ИС, действующими от имени пользователей) определенных операций над объектами (пассивными сущностями). Монитор проверяет каждое обращение пользователя к программам или данным на предмет согласованности с набором действий, допустимых для пользователя.

Монитор обращений должен обладать тремя качествами:

**Изолированность.** Необходимо предупредить возможность отслеживания работы монитора.

**Полнота**. Монитор должен вызываться при каждом обращении, не должно быть способов обойти его.

**Верифицируемость**. Монитор должен быть компактным, чтобы его можно было проанализировать и протестировать, будучи уверенным в полноте тестирования.

Реализация монитора обращений называется ядром безопасности. **Ядро безопасности** - это основа, на которой строятся все защитные механизмы. Помимо перечисленных выше свойств монитора обращений, ядро должно гарантировать собственную неизменность.

Границу доверенной вычислительной базы называют **периметром безопасности**. Как уже указывалось, компоненты, лежащие вне периметра безопасности, вообще говоря, могут не быть доверенными. С развитием распределенных систем понятию "периметр безопасности" все чаще придают другой смысл, имея в виду границу владений определенной организации. То, что находится внутри владений, считается доверенным, а то, что вне, - нет.

#### 1.1.2. Механизмы безопасности

Согласно "Оранжевой книге", политика безопасности должна обязательно включать в себя следующие элементы:

* произвольное управление доступом;
* безопасность повторного использования объектов;
* метки безопасности;
* принудительное управление доступом.

**Произвольное управление доступом (называемое иногда дискреционным)** - это метод разграничения доступа к объектам, основанный на учете личности субъекта или группы, в которую субъект входит. Произвольность управления состоит в том, что некоторое лицо (обычно владелец объекта) может по своему усмотрению предоставлять другим субъектам или отбирать у них права доступа к объекту.

**Безопасность повторного использования объектов**- важное дополнение средств управления доступом, предохраняющее от случайного или преднамеренного извлечения конфиденциальной информации из "мусора". Безопасность повторного использования должна гарантироваться для областей оперативной памяти (в частности, для буферов с образами экрана, расшифрованными паролями и т.п.), для дисковых блоков и магнитных носителей в целом.

Как мы указывали ранее, современный объектно-ориентированный подход резко сужает область действия данного элемента безопасности, затрудняет его реализацию. То же верно и для интеллектуальных устройств, способных буферизовать большие объемы данных.

Для реализации принудительного управления доступом с субъектами и объектами ассоциируются метки безопасности. Метка субъекта описывает его благонадежность, метка объекта - степень конфиденциальности содержащейся в нем информации.

Согласно "Оранжевой книге", метки безопасности состоят из двух частей - уровня секретности и списка категорий. Уровни секретности образуют упорядоченное множество, категории - неупорядоченное. Назначение последних - описать предметную область, к которой относятся данные.

**Принудительное (или мандатное) управление** доступом основано на сопоставлении меток безопасности субъекта и объекта.

Субъект может читать информацию из объекта, если уровень секретности субъекта не ниже, чем у объекта, а все категории, перечисленные в метке безопасности объекта, присутствуют в метке субъекта. В таком случае говорят, что метка субъекта доминирует над меткой объекта. Смысл сформулированного правила понятен - читать можно только то, что положено.

Субъект может записывать информацию в объект, если метка безопасности объекта доминирует над меткой субъекта. В частности, "конфиденциальный" субъект может записывать данные в секретные файлы, но не может - в несекретные (разумеется, должны также выполняться ограничения на набор категорий).

Описанный способ управления доступом называется принудительным, поскольку он не зависит от воли субъектов (даже системных администраторов). После того, как зафиксированы метки безопасности субъектов и объектов, оказываются зафиксированными и права доступа.

Если понимать политику безопасности узко, то есть как правила разграничения доступа, то механизм подотчетности является дополнением подобной политики. Цель подотчетности - в каждый момент времени знать, кто работает в системе и что делает. Средства подотчетности делятся на три категории:

* идентификация и аутентификация;
* предоставление доверенного пути;
* анализ регистрационной информации.

Обычный способ идентификации - ввод имени пользователя при входе в систему. Стандартное средство проверки подлинности (аутентификации) пользователя - пароль.

Доверенный путь связывает пользователя непосредственно с доверенной вычислительной базой, минуя другие, потенциально опасные компоненты ИС. Цель предоставления доверенного пути - дать пользователю возможность убедиться в подлинности обслуживающей его системы.

Анализ регистрационной информации (аудит) имеет дело с действиями (событиями**), так** или иначе затрагивающими безопасность системы.

Если фиксировать все события, объем регистрационной информации, скорее всего, будет расти слишком быстро, а ее эффективный анализ станет невозможным. "Оранжевая книга" предусматривает наличие средств выборочного протоколирования, как в отношении пользователей (внимательно следить только за подозрительными), так и в отношении событий.

Переходя к пассивным аспектам защиты, укажем, что в "Оранжевой книге" рассматривается два вида гарантированности - операционная и технологическая. Операционная гарантированность относится к архитектурным и реализационным аспектам системы, в то время как технологическая - к методам построения и сопровождения.

Операционная гарантированность включает в себя проверку следующих элементов:

* архитектура системы;
* целостность системы;
* проверка тайных каналов передачи информации;
* доверенное администрирование;
* доверенное восстановление после сбоев.

Операционная гарантированность - это способ убедиться в том, что архитектура системы и ее реализация действительно реализуют избранную политику безопасности.

Технологическая гарантированность охватывает весь жизненный цикл системы, то есть периоды проектирования, реализации, тестирования, продажи и сопровождения. Все перечисленные действия должны выполняться в соответствии с жесткими стандартами, чтобы исключить утечку информации и нелегальные "закладки".

#### 1.1.3. Классы безопасности

"Критерии ..." Министерства обороны США открыли путь к ранжированию информационных систем по степени доверия безопасности.

В "Оранжевой книге" определяется четыре уровня доверия - D, C, B и A. Уровень D предназначен для систем, признанных неудовлетворительными. По мере перехода от уровня C к A к системам предъявляются все более жесткие требования. Уровни C и B подразделяются на классы (C1, C2, B1, B2, B3) с постепенным возрастанием степени доверия.

Всего имеется шесть классов безопасности - C1, C2, B1, B2, B3, A1. Чтобы в результате процедуры сертификации систему можно было отнести к некоторому классу, ее политика безопасности и уровень гарантированности должны удовлетворять заданным требованиям, из которых мы упомянем лишь важнейшие.

*Класс C1:*

* доверенная вычислительная база должна управлять доступом именованных пользователей к именованным объектам;
* пользователи должны идентифицировать себя, прежде чем выполнять какие-либо иные действия, контролируемые доверенной вычислительной базой. Для аутентификации должен использоваться какой-либо защитный механизм, например пароли. Аутентификационная информация должна быть защищена от несанкционированного доступа;
* доверенная вычислительная база должна поддерживать область для собственного выполнения, защищенную от внешних воздействий (в частности, от изменения команд и/или данных) и от попыток слежения за ходом работы;
* должны быть в наличии аппаратные и/или программные средства, позволяющие периодически проверять корректность функционирования аппаратных и микропрограммных компонентов доверенной вычислительной базы;
* защитные механизмы должны быть протестированы на предмет соответствия их поведения системной документации. Тестирование должно подтвердить, что у неавторизованного пользователя нет очевидных способов обойти или разрушить средства защиты доверенной вычислительной базы;
* должны быть описаны подход к безопасности, используемый производителем, и применение этого подхода при реализации доверенной вычислительной базы.

*Класс C2 (в дополнение к C1):*

* права доступа должны гранулироваться с точностью до пользователя. Все объекты должны подвергаться контролю доступа;
* при выделении хранимого объекта из пула ресурсов доверенной вычислительной базы необходимо ликвидировать все следы его использования;
* каждый пользователь системы должен уникальным образом идентифицироваться. Каждое регистрируемое действие должно ассоциироваться с конкретным пользователем;
* доверенная вычислительная база должна создавать, поддерживать и защищать журнал регистрационной информации, относящейся к доступу к объектам, контролируемым базой;
* тестирование должно подтвердить отсутствие очевидных недостатков в механизмах изоляции ресурсов и защиты регистрационной информации.

*Класс B1 (в дополнение к C2):*

* доверенная вычислительная база должна управлять метками безопасности, ассоциируемыми с каждым субъектом и хранимым объектом;
* доверенная вычислительная база должна обеспечить реализацию принудительного управления доступом всех субъектов ко всем хранимым объектам;
* доверенная вычислительная база должна обеспечивать взаимную изоляцию процессов путем разделения их адресных пространств;
* группа специалистов, полностью понимающих реализацию доверенной вычислительной базы, должна подвергнуть описание архитектуры, исходные и объектные коды тщательному анализу и тестированию;
* должна существовать неформальная или формальная модель политики безопасности, поддерживаемой доверенной вычислительной базой.

*Класс B2 (в дополнение к B1):*

* снабжаться метками должны все ресурсы системы (например, ПЗУ), прямо или косвенно доступные субъектам;
* к доверенной вычислительной базе должен поддерживаться доверенный коммуникационный путь для пользователя, выполняющего операции начальной идентификации и аутентификации;
* должна быть предусмотрена возможность регистрации событий, связанных с организацией тайных каналов обмена с памятью;
* доверенная вычислительная база должна быть внутренне структурирована на хорошо определенные, относительно независимые модули;
* системный архитектор должен тщательно проанализировать возможности организации тайных каналов обмена с памятью и оценить максимальную пропускную способность каждого выявленного канала;
* должна быть продемонстрирована относительная устойчивость доверенной вычислительной базы к попыткам проникновения;
* модель политики безопасности должна быть формальной. Для доверенной вычислительной базы должны существовать описательные спецификации верхнего уровня, точно и полно определяющие ее интерфейс;
* в процессе разработки и сопровождения доверенной вычислительной базы должна использоваться система конфигурационного управления, обеспечивающая контроль изменений в описательных спецификациях верхнего уровня, иных архитектурных данных, реализационной документации, исходных текстах, работающей версии объектного кода, тестовых данных и документации;
* тесты должны подтверждать действенность мер по уменьшению пропускной способности тайных каналов передачи информации.

*Класс B3 (в дополнение к B2):*

* для произвольного управления доступом должны обязательно использоваться списки управления доступом с указанием разрешенных режимов;
* должна быть предусмотрена возможность регистрации появления или накопления событий, несущих угрозу политике безопасности системы. Администратор безопасности должен немедленно извещаться о попытках нарушения политики безопасности, а система, в случае продолжения попыток, должна пресекать их наименее болезненным способом;
* доверенная вычислительная база должна быть спроектирована и структурирована таким образом, чтобы использовать полный и концептуально простой защитный механизм с точно определенной семантикой;
* процедура анализа должна быть выполнена для временных тайных каналов;
* должна быть специфицирована роль администратора безопасности. Получить права администратора безопасности можно только после выполнения явных, протоколируемых действий;
* должны существовать процедуры и/или механизмы, позволяющие произвести восстановление после сбоя или иного нарушения работы без ослабления защиты;
* должна быть продемонстрирована устойчивость доверенной вычислительной базы к попыткам проникновения.

*Класс A1 (в дополнение к B3):*

* тестирование должно продемонстрировать, что реализация доверенной вычислительной базы соответствует формальным спецификациям верхнего уровня;
* помимо описательных, должны быть представлены формальные спецификации верхнего уровня. Необходимо использовать современные методы формальной спецификации и верификации систем;
* механизм конфигурационного управления должен распространяться на весь жизненный цикл и все компоненты системы, имеющие отношение к обеспечению безопасности;
* должно быть описано соответствие между формальными спецификациями верхнего уровня и исходными текстами.

Такова классификация, введенная в "Оранжевой книге". Коротко ее можно сформулировать так:

* уровень C - произвольное управление доступом;
* уровень B - принудительное управление доступом;
* уровень A - верифицируемая безопасность.

Конечно, в адрес "Критериев ..." можно высказать целый ряд серьезных замечаний (таких, например, как полное игнорирование проблем, возникающих в распределенных системах). Тем не менее, следует подчеркнуть, что публикация "Оранжевой книги" без всякого преувеличения стала эпохальным событием в области информационной безопасности. Появился общепризнанный понятийный базис, без которого даже обсуждение проблем ИБ было бы затруднительным.

Отметим, что огромный идейный потенциал "Оранжевой книги" пока во многом остается невостребованным. Прежде всего это касается концепции технологической гарантированности, охватывающей весь жизненный цикл системы - от выработки спецификаций до фазы эксплуатации. При современной технологии программирования результирующая система не содержит информации, присутствующей в исходных спецификациях, теряется информация о семантике программ. Важность данного обстоятельства мы планируем продемонстрировать далее, в лекции об управлении доступом.

#### 1.2. Информационная безопасность распределенных систем. Рекомендации X.800

##### 1.2.1. Сетевые сервисы безопасности

Следуя скорее исторической, чем предметной логике, мы переходим к рассмотрению технической спецификации X.800, появившейся немногим позднее "Оранжевой книги", но весьма полно и глубоко трактующей вопросы информационной безопасности распределенных систем.

Рекомендации X.800 - документ довольно обширный. Мы остановимся на специфических сетевых функциях (сервисах) безопасности, а также на необходимых для их реализации защитных механизмах.

Выделяют следующие сервисы безопасности и исполняемые ими роли:

**Аутентификация.** Данный сервис обеспечивает проверку подлинности партнеров по общению и проверку подлинности источника данных. Аутентификация партнеров по общению используется при установлении соединения и, быть может, периодически во время сеанса. Она служит для предотвращения таких угроз, как маскарад и повтор предыдущего сеанса связи. Аутентификация бывает односторонней (обычно клиент доказывает свою подлинность серверу) и двусторонней (взаимной).

**Управление доступом**. Обеспечивает защиту от несанкционированного использования ресурсов, доступных по сети.

**Конфиденциальность данных**. Обеспечивает защиту от несанкционированного получения информации. Отдельно упомянем конфиденциальность трафика (это защита информации, которую можно получить, анализируя сетевые потоки данных).

**Целостность данных** подразделяется на подвиды в зависимости от того, какой тип общения используют партнеры - с установлением соединения или без него, защищаются ли все данные или только отдельные поля, обеспечивается ли восстановление в случае нарушения целостности.

**Неотказуемость** (невозможность отказаться от совершенных действий) обеспечивает два вида услуг: неотказуемость с подтверждением подлинности источника данных и неотказуемость с подтверждением доставки. Побочным продуктом неотказуемости является аутентификация источника данных.

В следующей таблице указаны уровни эталонной семиуровневой модели OSI, на которых могут быть реализованы функции безопасности. Отметим, что прикладные процессы, в принципе, могут взять на себя поддержку всех защитных сервисов.

Табл.1. Распределение функций безопасности по уровням эталонной семиуровневой модели OSI

Функции безопасности

Уровень

1

2

3

4

5

6

7

Аутентификация

-

-

+

+

-

-

+

Управление доступом

-

-

+

+

-

-

+

Конфиденциальность соединения

-

+

+

+

-

+

+

Конфиденциальность вне соединения

-

+

+

+

-

+

+

Избирательная конфиденциальность

-

-

-

-

-

+

+

Конфиденциальность трафика

+

-

+

-

-

-

+

Целостность с восстановлением

-

-

-

+

-

-

+

Целостность без восстановления

-

-

+

+

-

-

+

Избирательная целостность

-

-

-

-

-

-

+

Целостность вне соединения

-

-

+

+

-

-

+

Неотказуемость

-

-

-

-

-

-

+

"+" данный уровень может предоставить функцию безопасности;

"-" данный уровень не подходит для предоставления функции безопасности.

##### 1.2.2. Сетевые механизмы безопасности

Для реализации сервисов (функций) безопасности могут использоваться следующие механизмы и их комбинации:

* шифрование;
* электронная цифровая подпись;
* механизмы управления доступом. Могут располагаться на любой из участвующих в общении сторон или в промежуточной точке;
* механизмы контроля целостности данных. В рекомендациях X.800 различаются два аспекта целостности: целостность отдельного сообщения или поля информации и целостность потока сообщений или полей информации. Для проверки целостности потока сообщений (то есть для защиты от кражи, переупорядочивания, дублирования и вставки сообщений) используются порядковые номера, временные штампы, криптографическое связывание или иные аналогичные приемы;
* механизмы аутентификации. Согласно рекомендациям X.800, аутентификация может достигаться за счет использования паролей, личных карточек или иных устройств аналогичного назначения, криптографических методов, устройств измерения и анализа биометрических характеристик;
* механизмы дополнения трафика;
* механизмы управления маршрутизацией. Маршруты могут выбираться статически или динамически. Оконечная система, зафиксировав неоднократные атаки на определенном маршруте, может отказаться от его использования. На выбор маршрута способна повлиять метка безопасности, ассоциированная с передаваемыми данными;
* механизмы нотаризации. Служат для заверения таких коммуникационных характеристик, как целостность, время, личности отправителя и получателей. Заверение обеспечивается надежной третьей стороной, обладающей достаточной информацией. Обычно нотаризация опирается на механизм электронной подписи.

В следующей таблице сведены сервисы (функции) и механизмы безопасности. Таблица показывает, какие механизмы (по отдельности или в комбинации с другими) могут использоваться для реализации той или иной функции.

##### 1.2.3.Администрирование средств безопасности

**Администрирование средств** безопасности включает в себя распространение информации, необходимой для работы сервисов и механизмов безопасности, а также сбор и анализ информации об их функционировании. Примерами могут служить распространение **криптографических ключей**, установка значений параметров защиты, ведение регистрационного журнала и т.п.

Табл. 2. Взаимосвязь функций и механизмов

**ФУНКЦИИ**

**МЕХАНИЗМЫ**

Шифрование

Электронная подпись

Управление доступом

Целостность

Аутентификация

Дополнение трафика

Управление маршрутизацией

Нотаризация

Аутентификация партнёров

+

+

-

-

+

-

-

-

Аутентификация источника

+

+

-

-

-

-

-

-

Управление доступом

-

-

+

-

-

-

-

-

Конфиденциальность

+

-

+

-

-

-

+

-

Избирательная конфиденциальность

+

-

-

-

-

-

-

-

Конфиденциальность трафика

+

-

-

-

-

+

+

-

Целостность соединения

+

-

-

+

-

-

-

-

Целостность вне соединения

+

+

-

+

-

-

-

-

Неотказуемость

-

+

-

+

-

-

-

+

"+" механизм пригоден для реализации данной функцию безопасности;

"-" механизм не преднозначен для реализации данной функции безопасности.

Концептуальной основой администрирования является информационная база управления безопасностью. Эта база может не существовать как единое (распределенное) хранилище, но каждая из оконечных систем должна располагать информацией, необходимой для реализации избранной политики безопасности.

Согласно рекомендациям X.800, усилия администратора средств безопасности должны распределяться по трем направлениям:

* администрирование информационной системы в целом;
* администрирование сервисов безопасности;
* администрирование механизмов безопасности.

Среди действий, относящихся к ИС в целом, отметим обеспечение актуальности политики безопасности, взаимодействие с другими административными службами, реагирование на происходящие события, аудит и безопасное восстановление.

Администрирование сервисов безопасности включает в себя определение защищаемых объектов, выработку правил подбора механизмов безопасности (при наличии альтернатив), комбинирование механизмов для реализации сервисов, взаимодействие с другими администраторами для обеспечения согласованной работы.

Обязанности администратора механизмов безопасности определяются перечнем задействованных механизмов. Типичный список таков:

* управление ключами (генерация и распределение);
* управление шифрованием (установка и синхронизация криптографических параметров). К управлению шифрованием можно отнести и администрирование механизмов электронной подписи. Управление целостностью, если оно обеспечивается криптографическими средствами, также тяготеет к данному направлению;
* администрирование управления доступом (распределение информации, необходимой для управления - паролей, списков доступа и т.п.);
* управление аутентификацией (распределение информации, необходимой для аутентификации - паролей, ключей и т.п.);
* управление дополнением трафика (выработка и поддержание правил, задающих характеристики дополняющих сообщений - частоту отправки, размер и т.п.);
* управление маршрутизацией (выделение доверенных путей);
* управление нотаризацией (распространение информации о нотариальных службах, администрирование этих служб).

Мы видим, что администрирование средств безопасности в распределенной ИС имеет много особенностей по сравнению с централизованными системами.

#### 1.3. Стандарт ISO/IEC 15408 "Критерии оценки безопасности информационных технологий"

##### 1.3.1.Основные понятия

Мы возвращаемся к теме оценочных стандартов, приступая к рассмотрению самого полного и современного среди них - "Критериев оценки безопасности информационных технологий" (издан 1 декабря 1999 года). Этот международный стандарт стал итогом почти десятилетней работы специалистов нескольких стран, он вобрал в себя опыт существовавших к тому времени документов национального и межнационального масштаба.

По историческим причинам данный стандарт часто называют "Общими критериями" (или даже ОК). Мы также будем использовать это сокращение.

"Общие критерии" на самом деле являются метастандартом, определяющим инструменты оценки безопасности ИС и порядок их использования. В отличие от "Оранжевой книги", ОК не содержат предопределенных "классов безопасности". Такие классы можно строить, исходя из требований безопасности, существующих для конкретной организации и/или конкретной информационной системы.

С программистской точки зрения ОК можно считать набором библиотек, помогающих писать содержательные "программы" - задания по безопасности, типовые профили защиты и т.п. Программисты знают, насколько хорошая библиотека упрощает разработку программ, повышает их качество. Без библиотек, "с нуля", программы не пишут уже очень давно; оценка безопасности тоже вышла на сопоставимый уровень сложности, и "Общие критерии" предоставили соответствующий инструментарий.

Важно отметить, что требования могут быть параметризованы, как и полагается библиотечным функциям.

Как и "Оранжевая книга", ОК содержат два основных вида требований безопасности:

* функциональные, соответствующие активному аспекту защиты, предъявляемые к функциям безопасности и реализующим их механизмам;
* требования доверия, соответствующие пассивному аспекту, предъявляемые к технологии и процессу разработки и эксплуатации.

Требования безопасности предъявляются, а их выполнение проверяется для определенного объекта оценки - аппаратно-программного продукта или информационной системы.

Очень важно, что безопасность в ОК рассматривается не статично, а в привязке к жизненному циклу объекта оценки. Выделяются следующие этапы:

* определение назначения, условий применения, целей и требований безопасности;
* проектирование и разработка;
* испытания, оценка и сертификация;
* внедрение и эксплуатация.

В ОК объект оценки рассматривается в контексте среды безопасности, которая характеризуется определенными условиями и угрозами.

В свою очередь, угрозы характеризуются следующими параметрами:

* источник угрозы;
* метод воздействия;
* уязвимые места, которые могут быть использованы;
* ресурсы (активы), которые могут пострадать.

Уязвимые места могут возникать из-за недостатка в:

* требованиях безопасности;
* проектировании;
* эксплуатации.

Слабые места по возможности следует устранить, минимизировать или хотя бы постараться ограничить возможный ущерб от их преднамеренного использования или случайной активизации.

С точки зрения технологии программирования в ОК использован устаревший библиотечный (не объектный) подход. Чтобы, тем не менее, структурировать пространство требований, в "Общих критериях" введена иерархия**класс-семейство**-**компонент-элемент.**

**Классы**определяют наиболее общую, "предметную" группировку требований (например, функциональные требования подотчетности).

**Семейства** в пределах класса различаются по строгости и другим нюансам требований.

**Компонент** - минимальный набор требований, фигурирующий как целое.

**Элемент** - неделимое требование.

Как и между библиотечными функциями, между компонентами ОК могут существовать зависимости. Они возникают, когда компонент сам по себе недостаточен для достижения цели безопасности. Вообще говоря, не все комбинации компонентов имеют смысл, и понятие зависимости в какой-то степени компенсирует недостаточную выразительность библиотечной организации, хотя и не заменяет объединение функций в содержательные объектные интерфейсы.

Как указывалось выше, с помощью библиотек могут формироваться два вида нормативных документов: профиль защиты и задание по безопасности.

Профиль защиты (ПЗ) представляет собой типовой набор требований, которым должны удовлетворять продукты и/или системы определенного класса (например, операционные системы на компьютерах в правительственных организациях).

Задание по безопасности содержит совокупность требований к конкретной разработке, выполнение которых обеспечивает достижение поставленных целей безопасности.

Выше мы отмечали, что в ОК нет готовых классов защиты. Сформировать классификацию в терминах "Общих критериев" - значит определить несколько иерархически упорядоченных (содержащих усиливающиеся требования) профилей защиты, в максимально возможной степени использующих стандартные функциональные требования и требования доверия безопасности.

Выделение некоторого подмножества из всего множества профилей защиты во многом носит субъективный характер. По целому ряду соображений (одним из которых является желание придерживаться объектно-ориентированного подхода) целесообразно, на наш взгляд, сформировать сначала отправную точку классификации, выделив базовый (минимальный) ПЗ, а дополнительные требования компоновать в функциональные пакеты.

Функциональный пакет - это неоднократно используемая совокупность компонентов, объединенных для достижения определенных целей безопасности. "Общие критерии" не регламентируют структуру пакетов, процедуры верификации, регистрации и т.п., отводя им роль технологического средства формирования ПЗ.

Базовый профиль защиты должен включать требования к основным (обязательным в любом случае) возможностям. Производные профили получаются из базового путем добавления необходимых пакетов расширения, то есть подобно тому, как создаются производные классы в объектно-ориентированных языках программирования.

##### 1.3.2. Функциональные требования

Функциональные требования сгруппированы на основе выполняемой ими роли или обслуживаемой цели безопасности. Всего в "Общих критериях" представлено 11 функциональных классов, 66 семейств, 135 компонентов. Это, конечно, значительно больше, чем число аналогичных сущностей в "Оранжевой книге".

Перечислим классы функциональных требований ОК:

* идентификация и аутентификация;
* защита данных пользователя;
* защита функций безопасности (требования относятся к целостности и контролю данных сервисов безопасности и реализующих их механизмов);
* управление безопасностью (требования этого класса относятся к управлению атрибутами и параметрами безопасности);
* аудит безопасности (выявление, регистрация, хранение, анализ данных, затрагивающих безопасность объекта оценки, реагирование на возможное нарушение безопасности);
* доступ к объекту оценки;
* приватность (защита пользователя от раскрытия и несанкционированного использования его идентификационных данных);
* использование ресурсов (требования к доступности информации);
* криптографическая поддержка (управление ключами);
* связь (аутентификация сторон, участвующих в обмене данными);
* доверенный маршрут/канал (для связи с сервисами безопасности).

Опишем подробнее два класса, демонстрирующие особенности современного подхода к ИБ.

Класс "Приватность" содержит 4 семейства функциональных требований.

**Анонимность.** Позволяет выполнять действия без раскрытия идентификатора пользователя другим пользователям, субъектам и/или объектам. Анонимность может быть полной или выборочной. В последнем случае она может относиться не ко всем операциям и/или не ко всем пользователям (например, у уполномоченного пользователя может оставаться возможность выяснения идентификаторов пользователей).

**Псевдонимность.** Напоминает анонимность, но при применении псевдонима поддерживается ссылка на идентификатор пользователя для обеспечения подотчетности или для других целей.

**Невозможность ассоциации.** Семейство обеспечивает возможность неоднократного использования информационных сервисов, но не позволяет ассоциировать случаи использования между собой и приписать их одному лицу. Невозможность ассоциации защищает от построения профилей поведения пользователей (и, следовательно, от получения информации на основе подобных профилей).

**Скрытность.**Требования данного семейства направлены на то, чтобы можно было использовать информационный сервис с сокрытием факта использования. Для реализации скрытности может применяться, например, широковещательное распространение информации, без указания конкретного адресата. Годятся для реализации скрытности и методы стеганографии, когда скрывается не только содержание сообщения (как в криптографии), но и сам факт его отправки.

Еще один показательный (с нашей точки зрения) класс функциональных требований - "Использование ресурсов", содержащий требования доступности. Он включает три семейства.

**Отказоустойчивость.** Требования этого семейства направлены на сохранение доступности информационных сервисов даже в случае сбоя или отказа. В ОК различаются активная и пассивная отказоустойчивость. Активный механизм содержит специальные функции, которые активизируются в случае сбоя. Пассивная отказоустойчивость подразумевает наличие избыточности с возможностью нейтрализации ошибок.

**Обслуживание по приоритетам**. Выполнение этих требований позволяет управлять использованием ресурсов так, что низкоприоритетные операции не могут помешать высокоприоритетным.

**Распределение ресурсов**. Требования направлены на защиту (путем применения механизма квот) от несанкционированной монополизации ресурсов.

Мы видим, что "Общие критерии" - очень продуманный и полный документ с точки зрения функциональных требований. В то же время, хотелось бы обратить внимание и на некоторые недостатки.

Первый мы уже отмечали - это отсутствие объектного подхода. Функциональные требования не сгруппированы в осмысленные наборы (объектные интерфейсы), к которым могло бы применяться наследование. Подобное положение, как известно из технологии программирования, чревато появлением слишком большого числа комбинаций функциональных компонентов, несопоставимых между собой.

В современном программировании ключевым является вопрос накопления и многократного использования знаний. Стандарты - одна из форм накопления знаний. Следование в ОК "библиотечному", а не объектному подходу сужает круг фиксируемых знаний, усложняет их корректное использование.

К сожалению, в "Общих критериях" отсутствуют архитектурные требования, что является естественным следствием избранного старомодного программистского подхода "снизу вверх". На наш взгляд, это серьезное упущение. Технологичность средств безопасности, следование общепризнанным рекомендациям по протоколам и программным интерфейсам, а также апробированным архитектурным решениям, таким как менеджер/агент, - необходимые качества изделий информационных технологий, предназначенных для поддержки критически важных функций, к числу которых, безусловно, относятся функции безопасности. Без рассмотрения интерфейсных аспектов системы оказываются нерасширяемыми и изолированными. Очевидно, с практической точки зрения это недопустимо. В то же время, обеспечение безопасности интерфейсов - важная задача, которую желательно решать единообразно.

##### 1.3.3. Требования доверия безопасности

Установление доверия безопасности, согласно "Общим критериям", основывается на активном исследовании объекта оценки.

Форма представления требований доверия, в принципе, та же, что и для функциональных требований. Специфика состоит в том, что каждый элемент требований доверия принадлежит одному из трех типов:

* действия разработчиков;
* представление и содержание свидетельств;
* действия оценщиков.

Всего в ОК 10 классов, 44 семейства, 93 компонента требований доверия безопасности. Перечислим классы:

* разработка (требования для поэтапной детализации функций безопасности от краткой спецификации до реализации);
* поддержка жизненного цикла (требования к модели жизненного цикла, включая порядок устранения недостатков и защиту среды разработки);
* тестирование;
* оценка уязвимостей (включая оценку стойкости функций безопасности);
* поставка и эксплуатация;
* управление конфигурацией;
* руководства (требования к эксплуатационной документации);
* поддержка доверия (для поддержки этапов жизненного цикла после сертификации);
* оценка профиля защиты;
* оценка задания по безопасности.

Применительно к требованиям доверия в "Общих критериях" сделана весьма полезная вещь, не реализованная, к сожалению, для функциональных требований. А именно, введены так называемые оценочные уровни доверия (их семь), содержащие осмысленные комбинации компонентов.

Оценочный уровень доверия 1 (начальный) предусматривает анализ функциональной спецификации, спецификации интерфейсов, эксплуатационной документации, а также независимое тестирование. Уровень применим, когда угрозы не рассматриваются как серьезные.

Оценочный уровень доверия 2, в дополнение к первому уровню, предусматривает наличие проекта верхнего уровня объекта оценки, выборочное независимое тестирование, анализ стойкости функций безопасности, поиск разработчиком явных уязвимых мест.

На третьем уровне ведется контроль среды разработки и управление конфигурацией объекта оценки.

На уровне 4 добавляются полная спецификация интерфейсов, проекты нижнего уровня, анализ подмножества реализации, применение неформальной модели политики безопасности, независимый анализ уязвимых мест, автоматизация управления конфигурацией. Вероятно, это самый высокий уровень, которого можно достичь при существующей технологии программирования и приемлемых затратах.

Уровень 5, в дополнение к предыдущим, предусматривает применение формальной модели политики безопасности, полуформальных функциональной спецификации и проекта верхнего уровня с демонстрацией соответствия между ними. Необходимо проведение анализа скрытых каналов разработчиками и оценщиками.

На уровне 6 реализация должна быть представлена в структурированном виде. Анализ соответствия распространяется на проект нижнего уровня.

Оценочный уровень 7 (самый высокий) предусматривает формальную верификацию проекта объекта оценки. Он применим к ситуациям чрезвычайно высокого риска.

На этом мы заканчиваем краткий обзор "Общих критериев".

#### 1.4. Гармонизированные критерии Европейских стран

Наше изложение "Гармонизированных критериев" основывается на версии 1.2, опубликованной в июне 1991 года от имени соответствующих органов четырех стран - Франции, Германии, Нидерландов и Великобритании.

Принципиально важной чертой Европейских Критериев является отсутствие требований к условиям, в которых должна работать информационная система. Так называемый спонсор, то есть организация, запрашивающая сертификационные услуги, формулирует цель оценки, то есть описывает условия, в которых должна работать система, возможные угрозы ее безопасности и предоставляемые ею защитные функции. Задача органа сертификации - оценить, насколько полно достигаются поставленные цели, то есть насколько корректны и эффективны архитектура и реализация механизмов безопасности в описанных спонсором условиях. Таким образом, в терминологии "Оранжевой книги", Европейские Критерии относятся к гарантированности безопасной работы системы. Требования к политике безопасности и наличию защитных механизмов не являются составной частью Критериев. Впрочем, чтобы облегчить формулировку цели оценки, Критерии содержат в качестве приложения описание десяти классов функциональности, типичных для правительственных и коммерческих систем.

Европейские Критерии рассматривают все основные составляющие информационной безопасности - конфиденциальность, целостность, доступность.

В Критериях проводится различие между системами и продуктами. Система - это конкретная аппаратно-программная конфигурация, построенная с вполне определенными целями и функционирующая в известном окружении. Продукт - это аппаратно-программный "пакет", который можно купить и по своему усмотрению встроить в ту или иную систему. Таким образом, с точки зрения информационной безопасности основное отличие между системой и продуктом состоит в том, что система имеет конкретное окружение, которое можно определить и изучить сколь угодно детально, а продукт должен быть рассчитан на использование в различных условиях.

Из практических соображений важно обеспечить единство критериев оценки продуктов и систем - например, чтобы облегчить оценку системы, составленной из ранее сертифицированных продуктов. По этой причине для систем и продуктов вводится единый термин - объект оценки.

Каждая система и/или продукт предъявляет свои требования к обеспечению конфиденциальности, целостности и доступности. Чтобы удовлетворить эти требования, необходимо предоставить соответствующий набор функций (сервисов) безопасности, таких как идентификация и аутентификация, управление доступом или восстановление после сбоев.

Сервисы безопасности реализуются посредством конкретных механизмов. Чтобы объекту оценки можно было доверять, необходима определенная степень уверенности в наборе функций и механизмов безопасности. Степень уверенности мы будем называть гарантированностью. Гарантированность может быть большей или меньшей в зависимости от тщательности проведения оценки.

Гарантированность затрагивает два аспекта - эффективность и корректность средств безопасности. При проверке эффективности анализируется соответствие между целями, сформулированными для объекта оценки, и имеющимся набором функций безопасности. Точнее говоря, рассматриваются вопросы адекватности функциональности, взаимной согласованности функций, простоты их использования, а также возможные последствия эксплуатации известных слабых мест защиты. Кроме того, в понятие эффективности входит способность механизмов защиты противостоять прямым атакам (мощность механизма). Определяются три градации мощности - базовая, средняя и высокая.

Под корректностью понимается правильность реализации функций и механизмов безопасности. В Критериях определяется семь возможных уровней гарантированности корректности - от E0 до E6 (в порядке возрастания). Уровень E0 означает отсутствие гарантированности. При проверке корректности анализируется весь жизненный цикл объекта оценки - от проектирования до эксплуатации и сопровождения.

Общая оценка системы складывается из минимальной мощности механизмов безопасности и уровня гарантированности корректности.

Гармонизированные критерии Европейских стран явились для своего времени весьма передовым стандартом, они создали предпосылки для появления "Общих критериев".

##### 1.5. Интерпретация "Оранжевой книги" для сетевых конфигураций

В 1987 году Национальным центром компьютерной безопасности США была опубликована интерпретация "Оранжевой книги" для сетевых конфигураций. Данный документ состоит из двух частей. Первая содержит собственно интерпретацию, во второй рассматриваются сервисы безопасности, специфичные или особенно важные для сетевых конфигураций.

В первой части вводится минимум новых понятий. Важнейшее из них - сетевая доверенная вычислительная база, распределенный аналог доверенной вычислительной базы изолированных систем. Сетевая доверенная вычислительная база формируется из всех частей всех компонентов сети, обеспечивающих информационную безопасность. Доверенная сетевая система должна обеспечивать такое распределение защитных механизмов, чтобы общая политика безопасности реализовывалась, несмотря на уязвимость коммуникационных путей и на параллельную, асинхронную работу компонентов.

Прямой зависимости между вычислительными базами компонентов, рассматриваемых как изолированные системы, и фрагментами сетевой вычислительной базы не существует. Более того, нет прямой зависимости и между уровнями безопасности отдельных компонентов и уровнем безопасности всей сетевой конфигурации. Например, в результате объединения двух систем класса B1, обладающих несовместимыми правилами кодирования меток безопасности, получается сеть, не удовлетворяющая требованию целостности меток. В качестве противоположного примера рассмотрим объединение двух компонентов, один из которых сам не обеспечивает протоколирование действий пользователя, но передает необходимую информацию другому компоненту, который и ведет протокол. В таком случае распределенная система в целом, несмотря на слабость компонента, удовлетворяет требованию подотчетности.

Чтобы понять суть положений, вошедших в первую часть, рассмотрим интерпретацию требований к классу безопасности C2. Первое требование к этому классу - поддержка произвольного управления доступом. Интерпретация предусматривает различные варианты распределения сетевой доверенной вычислительной базы по компонентам и, соответственно, различные варианты распределения механизмов управления доступом. В частности, некоторые компоненты, закрытые для прямого доступа пользователей, могут вообще не содержать подобных механизмов.

Интерпретация отличается от самих "Критериев" учетом динамичности сетевых конфигураций. Предусматривается наличие средств проверки подлинности и корректности функционирования компонентов перед их включением в сеть, наличие протокола взаимной проверки компонентами корректности функционирования друг друга, а также присутствие средств оповещения администратора о неполадках в сети. Сетевая конфигурация должна быть устойчива к отказам отдельных компонентов или коммуникационных путей.

Среди защитных механизмов в сетевых конфигурациях на первом месте стоит криптография, помогающая поддерживать как конфиденциальность, так и целостность. Следствием использования криптографических методов является необходимость реализации механизмов управления ключами.

Систематическое рассмотрение вопросов доступности является новшеством по сравнению не только с "Оранжевой книгой", но и с рекомендациями X.800. Сетевой сервис перестает быть доступным, когда пропускная способность коммуникационных каналов падает ниже минимально допустимого уровня или сервис не в состоянии обслуживать запросы. Удаленный ресурс может стать недоступным и вследствие нарушения равноправия в обслуживании пользователей. Доверенная система должна иметь возможность обнаруживать ситуации недоступности, уметь возвращаться к нормальной работе и противостоять атакам на доступность.

Для обеспечения непрерывности функционирования могут применяться следующие защитные меры:

* внесение в конфигурацию той или иной формы избыточности (резервное оборудование, запасные каналы связи и т.п.);
* наличие средств реконфигурирования для изоляции и/или замены узлов или коммуникационных каналов, отказавших или подвергшихся атаке на доступность;
* рассредоточенность сетевого управления, отсутствие единой точки отказа;
* наличие средств нейтрализации отказов (обнаружение отказавших компонентов, оценка последствий, восстановление после отказов);
* выделение подсетей и изоляция групп пользователей друг от друга.

Одним из важнейших в "Оранжевой книге" является понятие монитора обращений. Применительно к структурированию сетевой конфигурации можно сформулировать следующее утверждение, обеспечивающее достаточное условие корректности фрагментирования монитора обращений.

Пусть каждый субъект (то есть процесс, действующий от имени какого-либо пользователя) заключен внутри одного компонента и может осуществлять непосредственный доступ к объектам только в пределах этого компонента. Далее, пусть каждый компонент содержит свой монитор обращений, отслеживающий все локальные попытки доступа, и все мониторы реализуют согласованную политику безопасности. Пусть, наконец, коммуникационные каналы, связывающие компоненты, сохраняют конфиденциальность и целостность передаваемой информации. Тогда совокупность всех мониторов образует единый монитор обращений для всей сетевой конфигурации.

Данное утверждение является теоретической основой декомпозиции распределенной ИС в объектно-ориентированном стиле в сочетании с криптографической защитой коммуникаций.

##### 1.6. Руководящие документы Гостехкомиссии России

Гостехкомиссия России ведет весьма активную нормотворческую деятельность, выпуская Руководящие документы (РД), играющие роль национальных оценочных стандартов в области информационной безопасности. В качестве стратегического направления Гостехкомиссия России выбрала ориентацию на "Общие критерии", что можно только приветствовать.

В своем обзоре мы рассмотрим два важных, хотя и не новых, Руководящих документа - **Классификацию автоматизированных систем** (АС) по уровню **защищенности** от **несанкционированного доступа** (НСД) и аналогичную Классификацию **межсетевыхэкранов** (МЭ).

Согласно первому из них, устанавливается девять классов защищенности АС от НСД к информации.

Каждый класс характеризуется определенной минимальной совокупностью требований по защите.

Классы подразделяются на три группы, отличающиеся особенностями обработки информации в АС.

В пределах каждой группы соблюдается иерархия требований по защите в зависимости от ценности (конфиденциальности) информации и, следовательно, иерархия классов защищенности АС.

Третья группа классифицирует АС, в которых работает один пользователь, имеющий доступ ко всей информации АС, размещенной на носителях одного уровня конфиденциальности. Группа содержит два класса - 3Б и 3А.

Вторая группа классифицирует АС, в которых пользователи имеют одинаковые права доступа (полномочия) ко всей информации АС, обрабатываемой и (или) хранящейся на носителях различного уровня конфиденциальности.

Группа содержит два класса - 2Б и 2А.

Первая группа классифицирует многопользовательские АС, в которых одновременно обрабатывается и (или) хранится информация разных уровней конфиденциальности и не все пользователи имеют право доступа ко всей информации АС. Группа содержит пять классов - 1Д, 1Г, 1В, 1Б и 1А.

Сведем в таблицу требования ко всем девяти классам защищенности АС.

Табл. 3. Требования к защищенности автоматизированных систем

Подсистемы м требования

Классы

ЗБ

ЗА

2Б

2А

1Д

1Г

1В

1Б

1А

1. Подсистема управления досту-
пом

1.1. Идентификация. Проверка
подлинности и контроль доступа
субъектов в систему,

+

+

+

+

+

+

+

+

+

к терминалам, ЭВМ, узлам сети
ЭВМ, каналам связи, внешним
устройствам ЭВМ,

+

+

+

+

+

к программам,

+

+

+

+

+

к томам, каталогам, файлам, запи-
сям, полям записей.

+

+

+

+

+

1.2. Управление потоками инфор-
мации.

+

+

+

+

2. Подсистема регистрации и

учета

2.1.Регистрация и учет:

входа/выхода субъектов доступа

в/из системы (узла сети),

+

+

+

+

+

+

+

+

+

выдачи печатных (графических)
выходных документов,

+

+

+

+

+

+

запуска/завершения программ и
процессов (заданий, задач),

+

+

+

+

+

доступа программ к терминалам
ЭВМ, узлам сети ЭВМ, каналам
связи, внешним устройствам ЭВМ,
программам, каталогам, файлам,
записям, полям записей,

+

+

+

+

+

изменения полномочий субъектов
доступа,

+

+

+

создаваемых защищаемых объек-
тов доступа.

+

+

+

+

2.2. Учет носителей информации

+

+

+

+

+

+

+

+

+

2.3. Очистка (обнуление, обезли-
чивание) освобождаемых областей
оперативной памяти ЭВМ и внеш-
них накопителей

+

+

+

+

+

+

2.4. Сигнализация попыток нару-
шения защиты

+

+

+

3. Криптографическая подсисте-
ма

3.1. Шифрование конфиденциаль-
ной информации

+

+

+

3.2. Шифрование информации,
принадлежащей различным субъ-
ектам доступа (группам субъектов)
"на разных ключах

+

3.3. Использование аттестованных
(сертифицированных) криптогра-
фических средств

+

+

+

4. Подсистема обеспечения цело-
стности

4.1. Обеспечение целостности
программных средств и обрабаты-
ваемой информации

+

+

+

+

+

+

+

+

+

4.2. Физическая охрана средств
вычислительной техники и носи-
телей информации

+

+

+

+

+

+

+

+

+

4.3. Наличие администратора
(службы) зашиты информации в
АС

+

+

+

+

4.4. Периодическое тестирование
СЗИ НСД

+

+

+

+

+

+

+

+

+

4.5. Наличие средств восстановле-
ния СЗИ НСД

+

+

+

+

+

+

+■

+

+

4.6. Использование сертифициро-
ванных средств защиты

+

+

+

+

+

**1111111 L**

Обозначения: "+" - требование к данному классу присутствует;

"СЗИ НСД" - система защиты информации от
несанкционированного доступа.

По существу перед нами - минимум требований, которым необходимо следовать, чтобы обеспечить конфиденциальность информации. Целостность представлена отдельной подсистемой (номер 4), но непосредственно к интересующему нас предмету имеет отношение только пункт 4.1. Доступность (точнее, восстановление) предусмотрено только для самих средств защиты.

Переходя к рассмотрению второго РД Гостехкомиссии России - Классификации межсетевых экранов - укажем, что данный РД представляется нам принципиально важным, поскольку в нем идет речь не о целостном продукте или системе, а об отдельном сервисе безопасности, обеспечивающем межсетевое разграничение доступа.

Данный РД важен не столько содержанием, сколько самим фактом своего существования.

Основным критерием классификации МЭ служит протокольный уровень (в соответствии с эталонной семиуровневой моделью), на котором осуществляется фильтрация информации. Это понятно: чем выше уровень, тем больше информации на нем доступно и, следовательно, тем более тонкую и надежную фильтрацию можно реализовать.

Значительное внимание в РД уделено собственной безопасности служб обеспечения защиты и вопросам согласованного администрирования распределенных конфигураций.

**2. Порядок выполнения работы**

1.Ознакомиться со стандартами и спецификациями в области информационной безопасности .

2.Выполнить практическое задание.

3.Ответить на контрольные вопросы.

**3. Практические задания**

1. Разработать интерфейс пользователя «Оранжевая книга» как оценочный стандарт».

2. Разработать интерфейс пользователя «Информационная безопасность распределенных систем. Рекомендации X.800».

3. Разработать интерфейс пользователя «Стандарт ISO/IEC 15408 "Критерии оценки безопасности информационных технологий"

4. Разработать интерфейс пользователя «Гармонизированные критерии Европейских стран»

##### *5. Разработать интерфейс пользователя « Руководящие документы Гостехкомиссии России»*

**4. Контрольные вопросы**

**Вариант 1**

**1. Уровень безопасности С, согласно "Оранжевой книге",
характеризуется:**

* + произвольным управлением доступом
	+ принудительным управлением доступом
	+ верифицируемой безопасностью

**2. Согласно рекомендациям Х.800, аутентификация может
быть реализована на:**

* сетевом уровне
* транспортном уровне
* прикладном уровне

**3. "Общие критерии" содержат следующие виды
требований:**

* функциональные
* доверия безопасности
* экономической целесообразности

**Вариант 2**

**1. Уровень безопасности В, согласно "Оранжевой книге",
характеризуется:**

* произвольным управлением доступом
* принудительным управлением доступом
* верифицируемой безопасностью

**2. Согласно рекомендациям Х.800, целостность с
восстановлением может быть реализована на:**

* + сетевом уровне
	+ транспортном уровне
	+ прикладном уровне

**3. В число классов функциональных требований "Общих
критериев" входят:**

* + анонимность
	+ приватность
	+ связь

**Вариант 3**

**1. Уровень безопасности А, согласно "Оранжевой книге",
характеризуется:**

* + произвольным управлением доступом
	+ принудительным управлением доступом
	+ верифицируемой безопасностью

**2. Согласно рекомендациям Х.800, неотказуемость может
быть реализована на:**

* сетевом уровне
* транспортном уровне
* прикладном уровне

**3. В число классов требований доверия безопасности
"Общих критериев" входят:**

* разработка
* оценка профиля защиты
* сертификация

**Практическая работа №3. Основные виды технической и технологической документации.**

ЦЕЛЬ РАБОТЫ: получить практический опыт разработки и оформления подсистемы документирования комплекта технологических документов в САПР, их назначения и применения.

ЗАДАНИЕ: разработать и оформить электронный формы комплекта технологических документов «САПР ТП МО групповой детали».

Назначение и состав комплекта форм технологических документов.

Для оформления технологических процессов применяют соответствующую технологическую документацию. Единой системой технологической документации (ГОСТ 3.1102-81) предусматривается целый ряд технологических документов: маршрутная карта, карта эскизов, операционная карта, ведомость оснастки, ведомость материалов, ведомость технологических документов и т. д. Поэтому разработка технологического процесса механической обработки детали заканчивается составлением и оформлением комплекта документов технологического процесса [1, 4, 6]. Состав и формы карт, входящих в комплект документов, зависят от вида технологического процесса (единичный, типовой или групповой), типа производства и степени использования разработчиком средств вычислительной техники и автоматизированной системы управления производством. По степени детализации информации каждый из указанных видов технологических процессов предусматривает различные изложение содержания операции и комплектность документов.

Состав информационных блоков основной надписи форм технологических документов представлен на рис. -\_3\_.

В условиях единичного и мелкосерийного производств основным технологическим документом, с помощью которого технологический процесс доводится до рабочего места, является *маршрутная карта*(форма 1 по ГОСТ 3.1118-82 «Формы и правила оформления маршрутных карт»), дополняемая чертежом детали или операционным эскизом. Описание содержания технологических операций в маршрутных картах называется *маршрутным.*

В серийном и массовом производствах принято использовать *развернутые технологические процессы*с подробным описанием отдельных операций на операционных картах, составляемых совместно с картами эскизов. Для записи переходов операций механической обработки применяют определенные операционные карты (форма 3 по ГОСТ 3.1404-86 и др.), а для записи операций слесарных, слесарно-сборочных и электромонтажных — карты также определенной формы. Комплекс операционных карт, карт эскизов, различных ведомостей, составляющих развернутый технологический процесс, обычно сопровождается маршрутной картой. Изложение технологического процесса на операционных картах принято называть *пооперационным.*В *операционном технологическом процессе*маршрутная карта содержит только наименование всех операций в технологической последовательности, включая контроль и перемещение, перечень документов, применяемых при выполнении операции, технологическое оборудование и трудозатраты.

В *маршрутно-операционном технологическом процессе*предусматривается краткое описание содержания отдельных операций в маршрутной карте, а остальные операции оформляют на операционных картах.

*Карты эскизов*(операционные эскизы) — графические технологические документы, которые по своему назначению и содержанию заменяют (на данной операции) рабочий чертеж изделия (детали). Карта эскизов (КЭ) — основной графический документ, дающий наглядную информацию о выполняемой технологической операции.

***Маршрутная карта.***Маршрутная карта (МК) является основным и обязательным документом любого технологического процесса. Формы и правила оформления МК (рис. 2.8), применяемых при отработке технологических процессов изготовления или ремонта изделий в основном и вспомогательном производствах, регламентированы ГОСТ 3. 1118-82 «Формы и правила оформления маршрутных карт». К заполнению граф технологических документов предъявляются следующие требования.

1. Каждую строку мысленно делят по горизонтали пополам и информацию записывают в нижней ее части, оставляя верхнюю часть свободной для внесения изменений.

2. Для граф, выделенных утолщенными линиями, существуют три варианта заполнения:

а) графы заполняют кодами и обозначениями по соответствующим классификаторам и стандартам; вариант используется разработчиками, внедрившими автоматизированную систему управления производством;

б) информацию записывают в рекомендованном виде;

в) информацию дают в виде кодов с их расшифровкой.

Верх маршрутной карты (рис. 2.8, 2.9) также заполняют в соответствии с определенными требованиями. Графа 0 — указание организации. В графе 1 указывают наименование изделия (детали, сборочной единицы) по основному конструкторскому документу, например: «Вал шлицевой».

В графе 2 задают обозначение изделия по основному конструкторскому документу или код ступени классификации по конструкторскому классификатору, например 322705. Графа 3 указывает код классификационных группировок технологических признаков для типовых и групповых технологических процессов по технологическому классификатору [9, 10]. Графа 4 указывает код документа в соответствии с нижеприведенными кодами (ГОСТ 3. 1201-85):

первые две цифры — вид документации:

01 — комплект технологической документации;

10 — маршрутная карта;

20 — карта эскизов;

42 — ведомость оснастки;

44 — ведомость деталей к типовому (групповому) технологическому процессу (операции);

60 — операционная карта;

62 — карта наладки;

67 — карта кодирования информации;

третья цифра — вид технологического процесса (операции) по организации:

0 — без указания;

1 — единичный процесс (операция);

2 — типовой процесс (операция);

3 — групповой процесс (операция);

последние две цифры — вид технологического процесса по методу выполнения:

00 — без указания;

02, 03 — технический контроль;

04 — перемещение;

21 — обработка давлением;

41, 42 — обработка резанием;

50, 51 — термообработка.

П р и м е р. Маршрутная карта единичного процесса обработки резанием — 10141.ХХХХ [10 — маршрутная карта, 1 — единичный процесс (операция), 41 — обработка резанием]. Последние четыре разряда (ХХХХ) — резерв дополнительного обозначения по отраслевому классификатору. Карта с кодом 60202 указывает, что это операционная карта (код 60) типового процесса (код 2) технического контроля (код 02).

В графах 5 и 6 указывают общее количество листов документа (графа 5) и порядковый номер листа документа (графа 6). В графе 7 проставляют литеру, присвоенную технологическому документу, например: ОП — опытное производство. Графа 8 является графой для особых указаний.

Правила заполнения комплекта форм технологических документов.

***Служебные символы,***Для изложения технологических процессов в маршрутной карте используют способ заполнения, при котором информацию вносят построчно, при этом все строчки в МК нумеруют сверху вниз (см. рис. 2.8). Но каждую из строк индексируют в соответствии с заносимой в нее информацией. Каждому типу строки соответствует свой служебный символ: М, А, Б, К, О, Т, Р (табл.2.3). Служебные символы условно выражают состав информации, размещаемой в графах строки документа, и предназначены для обработки содержащейся информации средствами механизации и автоматизации. Простановка служебных символов является обязательной в любом случае. В качестве обозначения служебных символов приняты прописные буквы русского алфавита, проставляемые перед номером соответствующей строки. Указание соответствующих служебных символов для типов строк в зависимости от размещаемого состава информации в графах маршрутной карты следует выполнять в соответствии с таблицей.

Служебные символы для технологических документов

|  |  |  |
| --- | --- | --- |
|  | Служебный символ | Информация, вносимая в графы, расположенные в строке |
|  | М | Применяемый основной материал и исходная заготовка, исходные и комплектующие материалы, коды единицы величины, единицы нормирования, количество материала на изделие и нормы расхода |
|  | А | Номер цеха, участка, рабочего места, где выполняется операция; код и наименование операции |
|  | Б | Код, наименование оборудования, трудозатраты |
|  | К | Комплектация изделия (сборочной единицы) составными частями с указанием наименования деталей, сборочных единиц, их обозначений, кода единицы величины, единицы нормирования, количества материала на изделие и нормы расхода |
|  | О | Содержание операции (перехода) |
|  | Т | Применяемая при выполнении операции технологическая оснастка |
|  | Р | Режимы обработки |

*Служебный символ М.*Строки в маршрутной карте под символами М01 и М02 (см. рис. 2.8) задают информацию по заготовке (детали): наименование, сортамент, размер и марка материала, обозначение стандарта, технических условий. Запись (графа 34) выполняют на уровне одной строки с применением косой черты «/», например: Лист БОН-2,5x1000x2500 ГОСТ 19903-74/Ш-1У В ст. 3 ГОСТ 14637-79, или Круг В25 ГОСТ 2590-71/45 ГОСТ 1050-74, или Сталь 45X1 ГОСТ 4543-87/Штамповка.

Строка ниже определяет наименование (буквенными кодами) полей для строки М02, в которой последовательно записывают (в клетках под кодами):

код материала (под указанием *Код —*позиция *27*на рис. 2.8), пишется редко, ставится прочерк;

ЕВ — код единиц измерения массы, длины, площади и т. п. детали или заготовки (для массы, указанной в килограммах, — код 166; в граммах, — 163; в тоннах, — 168); допускается вместо кода указывать единицы измерения величины (позиция25 на рис. 2.8);

МД — масса детали по конструкторскому документу (позиция *29*на рис. 2.8); например: 0,72 (кг);

ЕН — единица нормирования, на которую установлены норма расхода материала или норма времени (позиция *30*на рис. 2.9); например: 1, 10, 100 (деталей);

*Н х —*норма расхода материала; например: 1,26 (кг) на 1 деталь (позиция *31*на рис. 2.8);

КИМ — коэффициент использования материала; например: 0,7 (позиция *32*на рис. 2.9);

код заготовки — код заготовки выбирают по классификатору (табл. 2.4); допускается указывать вид заготовки: отливка, прокат, штамповка и т. д.; например: 0950018 пр. (позиция 33 на рис. 2.9);

профиль и размеры — обозначение профиля и размеров заготовок; рекомендуется указывать толщину, ширину и длину, сторону квадрата или диаметр и длину; например: 0 35x3000 (позиция *35*на рис. 2.9); профиль допускается не указывать;

КД — количество деталей, изготавливаемых из одной заготовки; например: 10 (позиция *36*на рис. 2.8);

МЗ — масса заготовки; например: 12,6 (кг) (позиция 37 на рис. 2.8).

*Служебный символ А.*Строки в маршрутной карте под символом А (см. рис. 2.8 и 2.9) задают следующую информацию: номер цеха, в котором выполняется операция (позиция *23*на рис. 2.8), номер участка (позиция-24 на рис. 2.8), номер рабочего места (позиция *25*на рис. 2.8). Кроме этого, в строках с символом А указывают номер операции в технологической последовательности изготовления, контроля и перемещения (позиция *26*на рис. 2.8). Рекомендуемая нумерация операций: 000, 005, 010 и т. д. Далее задают код операции согласно классификатору технологических операций. После кода операции записывают ее наименование (позиция *22*на рис. 2.9). Всю информацию записывают в вертикальных столбцах карты, индексация которых определена в строчке с основной литерой А (позиция *А*на рис. 2.8 и 2.9).

Таким образом, информация со служебным символом А построчно будет записана, например, как показано на рис. 2.10.

Следует добавить, что в строках с символом А указывают обозначение документов, применяемых при выполнении данной операции, например: ИОТ — инструкция по охране труда. В табл. 2.5 выборочно приведены коды основных операций механической обработки и коды сопутствующего им оборудования. При наличии операции, выполняемой на станке с ПУ, к коду операции добавляют код 4103 или указывают соответствующий код, например: 4233 Токарная с ЧПУ (см. табл. 2.5).

*Служебный символ Б.*В строке с символом Б прежде всего записывают код и наименование оборудования, применяемого при выполнении заданной операции. Код включает в себя высшую (шесть первых цифр) и низшую (четыре цифры после точки) классификационные группировки. Выборочно коды оборудования указаны в табл. 2.5. Низшую группировку в МК иногда условно указывают знаком ХХХХ. Далее в строке с символом Б указывают информацию, связанную с трудозатратами и условиями работ (см. рис. 2.8 и 2.9). В МК допускается использовать сокращенную форму записи наименования операции и используемого оборудования (табл. 2.6).

СМ — код степени механизации труда (позиция *20*на рис. 2.8 и 2.9), указывают одной цифрой:

1 — наблюдение за работой автоматов;

2 — работа на машинах и автоматах;

3 — вручную при машинах и автоматах;

4 — вручную без машин и автоматов;

5 — вручную при наладке машин.

Проф. — код профессии (позиция *19*на рис. 2.9) согласно классификатору.

Р — разряд работы (позиция *18*на рис. 2.9), необходимый для выполнения операции. Код включает три цифры: первая — разряд работы по тарифно-квалификационному справочнику, две следующие — код формы и системы оплаты труда:

10 — сдельная форма оплаты труда;

11 — сдельная система оплаты труда прямая;

12 — сдельная система оплаты труда премиальная;

13 — сдельная система оплаты труда прогрессивная;

20 — повременная форма оплаты труда;

21 — повременная система оплаты труда простая;

22 — повременная система оплаты труда премиальная.

УТ — код условий труда (позиция 17 на рис. 2.9), состоящий из цифры — условия труда: 1 — нормальные; 2 — тяжелые и вредные; 3 — особо тяжелые, особо вредные — и буквы, указывающей вид нормы времени: Р — аналитически-расчетная; И — аналитически-исследовательская; X — хронометражная; О — опытно-статистическая.

КР — количество исполнителей, занятых при выполнении операции (позиция 16 на рис. 2.9).

КОИД — количество одновременно обрабатываемых заготовок при выполнении одной операции (позиция 15 на рис. 2.9).

ЕН — единица нормирования (позиция *14*на рис. 2.9), на которую установлены нормы расхода материала или норма времени; например: 1, 10, 100.

ОП — объем производственной партии в штуках (позиция *13*на рис. 2.9).

Кшт — коэффициент штучного времени при многостаночном обслуживании, зависящий от количества обслуживаемых станков (позиция *12*на рис. 2.9), например: 1 станок — Кшт = 1; 2 станка — Кшт = 0,65; 3 станка — Кшт = 0,48; 4 станка — Кшт = 0,39; 5 станков — Кщт = 0,35.

Тпз — подготовительно-заключительное время на операцию в минутах (позиция *11*на рис. 2.9).

Тшт — норма штучного времени на операцию в минутах (позиция *10*на рис. 2.9).

*Служебный символ Т.*При заполнении информации в строках, имеющих служебный символ Т, следует руководствоваться требованиями соответствующих классификаторов, государственных и отраслевых стандартов на кодирование (обозначения) и наименование технологической оснастки (табл. 2.8.). В строках с символом Т информацию о применяемой на операции технологической оснастке записывают в следующей последовательности: 1 — приспособления; 2 — вспомогательный инструмент; 3 — режущий инструмент; 4 — слесарно-монтажный инструмент; 5 — специальный инструмент; 6 — средства измерения. Разделение информации по каждому средству технологической оснастки следует выполнять через знак точку с запятой. Перед наименованием каждого элемента технологической оснастки указывают его код согласно классификаторам. При необходимости на записываемый элемент технологической оснастки указывают ГОСТ. Например, полная запись технологической оснастки (в строке с индексом Т) может быть такой:

*396131 Тиски машинные 7200-0010 ГОСТ 21167-85; 391855 Фреза торцевая 2214-ХХХХ 0160 210 ВК6М ГОСТ 24359-80-2; Оправка 6222-0034 040 ГОСТ 13785-80 (2 шт.).*

Но запись оснастки может быть и короче, все зависит от уровня и характера производства.

*Служебный символ О.*При заполнении информации в строках, имеющих служебный символ 0, следует руководствоваться правилами записи операций и переходов. Фрагмент маршрутной карты, в которой отражены технологические переходы, представлен на рис. 2.11. От приведенного выше он отличается тем, что за строка-ми с символом Т следуют строки с символом О, в которых последовательно, со своей нумерацией указаны переходы операции.

*Служебный символ Р,*При заполнении информации на строках, имеющих служебный символ Р, следует руководствоваться правилами записи режимов резания при записи операций и переходов (см. разд. Операционная карта).

Сводная таблица (табл. 2.9) поможет ориентироваться в записях МК.

***Операционная карта.***Структура построения операционной карты (ОК) идентична маршрутной. Большинство граф ОК соответствуют аналогичным графам маршрутной карты. Информацию по дополнительным графам следует вносить в соответствии с рис. 2.11. Запись содержания перехода следует выполнять в соответствии с рекомендациями табл. 2.10.

Запись информации в ОК выполняют также построчно с привязкой к соответствующим служебным символам (см. табл. 2.3). Указание единиц величин следует выполнять в заголовках или подзаголовках соответствующих граф. Допускается указывать единицы величин технологических режимов после их числовых значений; например: 40 мм; 0,2 мм/об; 36 мм/мин.

Указание данных по технологическим режимам следует выполнять в строках с символом *Р*после записи состава применяемой технологической оснастки, строки которой имеют символ *Т.*

При указании данных по технологической оснастке информацию следует записывать в следующей последовательности:

1) приспособления;

2) вспомогательный инструмент;

3) режущий инструмент;

4) средства измерения.

В целях разделения информации по группам технологической оснастки и поиска необходимой информации допускается перед указанием состава применять условное обозначения видов: приспособлений — ПР; вспомогательного инструмента — ВИ; режущего инструмента — РИ; средств измерений — СИ. Например: «СИ. АВВХХХ. Пробка024Н7-пр.». Универсальный мерительный инструмент в операционных картах, как правило, не указывают.

При описании содержания перехода при необходимости указывают данные по *Т0*(время операционное) и Тв (время вспомогательное). Это следует выполнять на уровне строки, где заканчивается описание содержания перехода под служебным символом «О».

Полную запись перехода делают при необходимости перечисления всех выдерживаемых размеров. Сокращенную запись используют при ссылке на условное обозначение конструктивного элемента обрабатываемого изделия. Данную запись выполняют при достаточной графической информации. Для промежуточных переходов, не имеющих графических иллюстраций, в содержании следует указывать исполнительные размеры с их предельными отклонениями и при необходимости шероховатость обработанной поверхности и другие технические требования. Например: «Точить поверхность 3, выдерживая (I = 40-Ю,34 и / = 100 + 0,4».

Переходы (основные и вспомогательные) нумеруют арабскими цифрами. В общем случае в содержание перехода включают:

1) ключевое слово, характеризующее метод обработки и выраженное глаголом в неопределенной форме (табл. 2.11);

2) наименование (существительное в винительном падеже) обрабатываемой поверхности, конструктивных элементов или предметов производства; например: «отверстие», «фаску», «канавку», «заготовку» и т. п.;

3) информацию о размерах обработки резанием или об их условных обозначениях, указанных на операционных эскизах арабскими цифрами в окружности диаметром 6-8 мм (табл. 2.12);

4) дополнительную информацию, отражающую количество одновременно или последовательно обрабатываемых поверхностей, характер обработки; например: «предварительно», «последовательно », « по копиру ».

Параметры шероховатости обрабатываемой поверхности указывают только обозначениями на операционном эскизе. Допускается указывать только в тексте (в строке «Содержание операций») информацию о параметре шероховатости предварительно обрабатываемых поверхностей (промежуточных переходов), если это нельзя указать на операционном эскизе; например: «фрезеровать предварительно поверхность 1, выдерживая высоту 70 + 0,5, К2 = 50».

Примеры полной и сокращенной записи содержания переходов обработки резанием приведены в табл.2.12.

В строке с символом Р приводят размеры обрабатываемых поверхностей: расчетный диаметр!) или ширину В и расчетную длину обработки Ь (позиции 4 и 6 на рис. 2.12), определяемую с учетом длин врезания и перебега. При этом учитывают наибольший диаметр, по которому рассчитывают скорость резания. При обработке сверлом, зенкером, разверткой, метчиком в графе «D» или «В» указывают диаметр инструмента. Глубину резания при обработке (и число рабочих ходов *i*) указывают (позиции 7 и 8 на рис. 2.12) в соответствии с условием обработки при переходе. Подачу S (позиция 9 на рис. 2.12) в операционной карте принимают в зависимости от вида обработки: для токарных работ — на один оборот заготовки (мм/об); для строгальных и долбежных — на один двойной ход стола или резца (мм/дв. ход); для сверлильных, расточных, резьбонарезных и других видов обработки отверстий с вращением инструмента — на один оборот шпинделя станка (мм/об). При фрезерных работах в графе 8 записывают две подачи: в числителе — подачу в минуту (мм/мин), а в знаменателе — подачу на зуб (мм/зуб).

При фрезеровании шпоночных пазов (с маятниковой подачей) двухперьевыми фрезами указывают вертикальную и продольную подачи: в числителе — вертикальную на двойной ход фрезы (мм/дв. ход), а в знаменателе — продольную в минуту (мм/мин). При круглом наружном шлифовании с продольной подачей и при шлифовании отверстий подачу обозначают также дробью: в числителе — продольную в долях ширины шлифовального круга на один оборот детали (мм/об), а в знаменателе — вертикальную (поперечную) на двойной ход стола (мм/дв. ход).

При шлифовании методом врезания задают только поперечную подачу на один оборот детали (мм/об), а при обработке плоскости торцом круга — вертикальную на оборот стола (при его вращении) или на двойной ход стола (мм/об, мм/дв. ход).

При шлифовании плоскости периферией круга в графе 5 записывают три подачи: продольную (мм/мин), вертикальную (мм/раб. ход) и поперечную, выражаемую в долях ширины круга (от 0,1 до 0,9Б) на двойной ход стола.

Для зубодолбежных станков в числителе приводят радиальную подачу на двойной ход долбяка — подачу врезания (мм/ дв. ход), а в знаменателе — круговую подачу на двойной ход долбяка — подачу обкатки (мм/дв. ход). Для зубофрезерных станков при обработке червячными фрезами зубчатых колес указывают подачу на один оборот заготовки (мм/об). При нарезании червячных колес методом радиальной подачи в графе 8 записывают радиальную подачу стола на один его оборот (мм/об), при нарезании методом тангенциальной подачи — осевую подачу фрезы на оборот стола (мм/об).

Частоту вращения шпинделя n (позиция 12 на рис. 2.12) задают обычно для всех станков в оборотах в минуту (об/мин). При круглом шлифовании записывают: в числителе — частоту вращения круга (об/мин), в знаменателе — частоту вращения детали (об/мин).

Скорость резания v (позиция 11 на рис. 2.12) рассчитывают по наибольшему диаметру обработки на данном переходе (м/мин). Для шлифовальных работ указывают скорость резания (м/с).

В графе Т0 (позиция 3 на рис. 2.12) записывают основное (машинное) время на переход с учетом затрат времени на врезание и перебег инструмента для всех видов механической обработки и на обратный ход для обработки на станках с возвратно-поступательным движением инструмента (строгальный, протяжной и т. п.).

В графе ТВ (позиция 5 на рис. 2.12) записывают вспомогательное время на переход, связанное с управлением станком и выполнением вспомогательных переходов и контролем.

Документы технического контроля. Операционные карты технического контроля по ГОСТ 3.1502-85 (форма 2). Информацию, вносимую в некоторые графы карты (рис. 2.13), записывают в соответствии с рекомендациями, приведенными в табл. 2.13. Остальные графы заполняют по аналогии с маршрутной и операционной картами.

При описании операций технического контроля следует применять полную или краткую форму записи содержания переходов. Полную форму записи следует выполнять на всю длину строки с включением граф «Объем и ПК» и «Т0/ТВ»; при этом должна быть предусмотрена возможность переноса информации на последующие строки. Данные по применяемым средствам измерений следует записывать всегда с новой строки.

Краткую форму записи надо применять только при проверке контролируемых размеров и других данных, выраженных числовыми значениями. В этом случае текстовую запись применять не следует, необходимо указать только соответствующие параметры; например: 047 ± 0,039.

Данные по применяемым средствам технологического оснащения следует записывать исходя из их возможностей, т. е. к каждому контролируемому размеру (параметру) или к группе контролируемых размеров (параметров). Графические изображения, сопровождаемые текстовые документы, если это необходимо, следует выполнять на форме карты эскизов по ГОСТ 3.1105-84.

Оформление документов на бумажных носителях, проектируемых с применением средств механизации и автоматизации. При проектировании технологических процессов с помощью ПЭВМ (ПК) их оформление должно соответствовать общим требованиям к формам и бланкам ТД, которые установлены ГОСТ 3.1104-81. Пример оформления карты технологического процесса на бумажном носителе с применением ПЭВМ приведен на рис. 2.14. Принцип записи технологической информации сохранен и выполнен с использованием служебных символов, но с некоторыми добавлениями и изменениями. Так, функции символа А (номер цеха, участка, рабочего места, где выполняется операция; код и наименование операции) выполняет символ В; вместо символа Б (код, наименование оборудования и информация по трудозатратам) введен символ Д (код, наименование оборудования), а информацию по трудозатратам записывают отдельно с символом Е. Отдельно используют символ Г — обозначение документов. Символы М, К, О, Т и Р используют в соответствии с их назначением, заданным им ранее.

В технологических документах, подготовленных с использованием систем САВ/САМ, также могут быть особенности, определенные схемой построения системы.

Естественно, что определенные требования предъявляются к оформлению ТД на типовые и групповые ТП, на обработку деталей на станках с ПУ (ЧПУ), на токарных автоматах и полуавтоматах и т. д..

Технологический процесс состоит из различных операций, поэтому при разработке ТП следует кодировать операции всех видов.



|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| № графы | Обозначение графы | Кол-во знаков | Содержание графы | Размер в пунктах |
| 1 | М | 5 | Обозначение служебного символа и порядковый номер строки. | 34,58 |
| 2 | - | 89 | Наименование, сортамент, размер и марка материала, ГОСТ, ТУ | 615,59 |
| 3 | Код | 13 | Код материала по классификатору. | 89,92 |
| 4 | ЕВ | 4 | Код единицы величины (массы, длины, площади и т. п.) детали, заготовки, материала по классификатору СОЕИ. Допускается указывать единицы измерения величины. | 27,67 |
| 5 | МД | 7 | Масса детали по конструкторскому документу. | 48,42 |
| 6 | ЕН | 6 | Единица нормирования, на которую установлена норма расхода материала или времени (1„ 10., 100 и т. д.) | 41,50 |
| 7 | Н. расх. | 7 | Норма расхода материала | 48,42 |
| 8 | КИМ | 5 | Коэффициент использования материала. | 34,58 |
| 9 | Код заготовки | 13 | Код заготовки по классификатору. Допускается указывать вид заготовки (отливка, прокат, поковка и т. п.). | 89,92 |
| 10 | Профиль и размеры | 21 | Профиль и размеры исходной заготовки. Информацию по размерам следует указывать исходя из условий имеющихся размеров заготовки (длины, ширины, высоты), например, 1000 Х 2500 Х 100. | 145,25 |
| 11 | КД | 6 | Количество деталей, изготовляемых из одной заготовки | 41,50 |
| 12 | МЗ | 7 | Масса заготовки. | 48,42 |
| 13 | - | 16 | Особые указания. Заполняется согласно отраслевыми нормативно-техническими документами (НТД). | 110,67 |

Рис. \_\_4\_\_\_. Состав (структура) граф содержащих информацию о материале и заготовке и обозначаемых символом «М».



|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| № графы | Обозначение графы | Кол-во знаков | Содержание графы | Размер в пунктах |
| 1 | А | 5 | Обозначение служебного символа и порядковый номер строки. | 34,58 |
| 2 | Цех | 4 | Номер (код) цеха, в котором выполняется операция | 27,67 |
| 3 | Уч. | 4 | Номер (код) участка, конвейера, поточной линии | 27,67 |
| 4 | РМ | 4 | Номер (код) рабочего места | 27,67 |
| 5 | Опер. | 5 | Номер операции (процесса) в технологической последовательности изготовления детали (включая контроль и перемещение) | 34,58 |
| 6 | Код, наименование операции | 29 | Код операции по технологическому классификатору, наименование операции | 200,59 |
| 7 | Обозначение документа | 59 | Обозначение документов, инструкций по охране труда, применяемых при выполнении данной операции. Состав документов следует указывать через разделительный знак «;» с допущением размещения информации на последующих строках | 408,09 |

Рис. \_\_5\_\_\_. Состав (структура) графы содержащей информацию об операции и обозначаемых символом «А».



|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| № графы | Обозначение графы | Кол-во знаков | Содержание графы | Размер в пунктах |
| 1 | Б | 5 | Обозначение служебного символа и порядковый номер строки. | 34,58 |
| 2 | Код, наименование оборудования | 45 | Код оборудования по классификатору, краткое наименование оборудования и инвентарный номер. | 311,25 |
| 3 | СМ | 4 | Степень механизации. Обязательность заполнения графы устанавливается отраслевыми НТД | 27,67 |
| 4 | Проф. | 7 | Код профессии по классификатору ОКПДТР | 48,42 |
| 5 | Р | 4 | Разряд работы, необходимый для выполнения операции по ОКПДТР | 27,67 |
| 6 | УТ | 5 | Код условий труда по классификатору ОКПДТР и код вида нормы | 34,58 |
| 7 | КР | 4 | Количество исполнителей, занятых при выполнении операции | 27,67 |
| 8 | КОИД | 5 | Количество одновременно обрабатываемых деталей. | 34,58 |
| 9 | ЕН | 6 | Ед. нормирования, на которую установлена норма расхода материала или времени (1, 10, 100 и т. д.) | 41,50 |
| 10 | Кшт. | 5 | Коэффициент штучного времени при многостаночном обслуживании | 34,58 |
| 11 | ОП | 5 | Объем производственной партии в штуках. | 34,58 |
| 12 | Тпз | 7 | Норма подготовительно-заключительного времени на операцию | 48,42 |
| 13 | Тшт. | 8 | Норма штучного времени на операцию | 55,33 |

Рис. \_\_6\_\_\_. Состав (структура) граф содержащих информацию об операции и обозначаемых символом «Б».



|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| № графы | Обозначение графы | Кол-во знаков | Содержание графы | Размер в пунктах |
| 1 | Р | 5 | Обозначение служебного символа и порядковый номер строки. | 34,58 |
| 2 | ПИ | 7 | Номер позиции инструментальной наладки. | 48,42 |
| 3 | D или В | 11 | Расчетный размер обрабатываемого диаметра (ширины) детали | 76,08 |
| 4 | L | 9 | Расчетный размер длины рабочего хода. | 62,25 |
| 5 | t | 5 | Глубина резания | 34,58 |
| 6 | I | 6 | Число проходов | 39,90 |
| 7 | S | 10 | Подача, мм/об | 69,17 |
| 8 | n | 7 | Число оборотов шпинделя в мин. | 48,42 |
| 9 | v | 8 | Скорость резания, м/мин | 55,33 |

Рис. \_7\_. Состав (структура) граф содержащих информацию о параметрах технологических переходов и обозначаемых символом «Р».



Рис 8 . Разметка листа КТП.

ПОРЯДОК ВЫПОЛНЕНИЯ РАБОТЫ.

1. В файле приложении Microsoft Office Excel 2003 на листе с КТП назначить параметры столбцов в соответствии со строкой 27 Рис. 8.
2. В файле приложении Microsoft Office Excel 2003 на листе с КТП последовательно объединить ячейки в соответствии со строками 14-25 Рис. 8.
3. Нанести соответствующие надписи ячейках.
4. Выделить группы ячеек утолщённой линией в соответствии с рис.8.
5. Скопировать сформированный лист в количестве 3 в данной книге и расположить их последовательно.
6. Удалить на первом листе КТП строки типа М, А, Б, Р.Преобразовать поле документа в Титульный лист и переименовать лист как Титульный (ТЛ).
7. Последующие листы переименовать как КТП1, КТП2.

КОНТРОЛЬНЫЕ ВОПРОСЫ:

1. Назначение форм комплекта технологических документов?
2. Состав информации в строках типа М, А, Б, Р?
3. Назначение и состав информации в основных блоках технологических документов?
4. Состав комплекта технологических документов, критерии его формирования?
5. Привести примеры производственных задач, использующих информацию содержащуюся в комплекте технологических документов ?

**Список литературы**

1. Дехтярь Г. М. Метрология, стандартизация и сертификация : учеб. пособие М.: КУРС, НИЦ ИНФРА-М 2016 - - https://znanium.com/bookread2.php?book=537788

2. В.Е. Эрастов Метрология, стандартизация и сертификация : учеб. пособие М. : ИНФРА-М 2017 - - https://znanium.com/bookread2.php?book=636240

3. Е.Б. Герасимова, Б.И. Герасимов Метрология, стандартизация и сертификация : учеб. пособие М. : ФОРУМ : ИНФРА-М 2017 - - http://znanium.com/catalog/product/767649

4. С.А. Любомудров, А.А. Смирнов, С.Б. Тарасов Метрология, стандартизация и сертификация: нормирование точности : учебник М. : ИНФРА-М 2017 - - http://znanium.com/catalog/product/900842

5. А.А. Иванов, А.И. Ковчик, А.С. Столяров Метрология, стандартизация и сертификация : учебник Москва : ИНФРА-М 2019 https://znanium.com/bookread2.php?book=1015886