**МИНИСТЕРСТВО НАУКИ И ВЫСШЕГО ОБРАЗОВАНИЯ РОССИЙСКОЙ ФЕДЕРАЦИИ**
**Федеральное государственное бюджетное образовательное учреждение высшего образования**
**«Кузбасский государственный технический университет имени Т. Ф. Горбачева»**

Кафедра металлорежущих станков и инструментов

Составитель
К. П. Петренко

# СТАНДАРТИЗАЦИЯ, СЕРТИФИКАЦИЯ И ТЕХНИЧЕСКОЕ ДОКУМЕНТИРОВАНИЕ

## Методические материалы

Рекомендованы цикловой методической комиссией
общепрофессиональных дисциплин
в качестве электронного издания
для использования в образовательном процессе

Кемерово 2018

Рецензенты

Коротков А. Н. – доктор технических наук, профессор, заведующий кафедрой металлорежущих станков и инструментов

Ушакова Е. С. – кандидат технических наук, председатель цикловой методической комиссии общепрофессиональных дисциплин.

**Петренко Константин Петрович**

**Стандартизация, сертификация и техническое документирование**: методические материалы [Электронный ресурс] для студентов специальности СПО 09.02.07 Информационные системы и программирование очной формы обучения / сост. К. П. Петренко; КузГТУ. – Электрон. издан. – Кемерово, 2018.

Приведено содержание практических и самостоятельных работ, материал, необходимый для успешного изучения дисциплины.

Назначение издания – помощь студентам в получении знаний по дисциплине «Стандартизация, сертификация и техническое документоведение» и организация практических и самостоятельных работ.

# СОДЕРЖАНИЕ

# Практическая работа №1

# НОРМАТИВНО-ПРАВОВЫЕ ДОКУМЕНТЫ И СТАНДАРТЫ В ОБЛАСТИ ЗАЩИТЫ ИНФОРМАЦИИ И ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

## 1. ЦЕЛЬ РАБОТЫ

Ознакомиться с нормативно-правовыми основами «информационной безопасности» в РФ, нормативными документами и ответственностью за нарушения информационной безопасности.

## 2. ТЕОРЕТИЧЕСКИЕ ПОЛОЖЕНИЯ

### 2.1. Правовые основы «информационной безопасности» общества

Законодательные меры в сфере информационной безопасности направлены на создание в стране законодательной базы, упорядочивающей и регламентирующей поведение субъектов и объектов информационных отношений, а также определяющей ответственность за нарушение установленных норм.

Работа по созданию нормативной базы предусматривает разработку новых или корректировку существующих законов, положений, постановлений и инструкций, а также создание действенной системы контроля над исполнением указанных документов. Необходимо отметить, что такая работа в последнее время ведется практически непрерывно, поскольку сфера информационных технологий развивается стремительно, соответственно появляются новые формы информационных отношений, существование которых должно быть определено законодательно.

Законодательная база в сфере информационной безопасности включает пакет:

- Федеральных законов;
- Указов Президента РФ;

- Постановлений Правительства РФ;
- Межведомственных руководящих документов и стандартов.

Основополагающими документами по информационной безопасности в РФ являются Конституция РФ и Концепция национальной безопасности.

В Конституции РФ гарантируется «тайна переписки, телефонных переговоров, почтовых, телеграфных и иных сообщений» (ст. 23, ч. 2), а также «право свободно искать, получать, передавать, производить и распространять информацию любым законным способом» (ст. 29, ч. 4). Кроме этого, Конституцией РФ «гарантируется свобода массовой информации» (ст. 29, ч. 5), т. е. массовая информация должна быть доступна гражданам.

Концепция национальной безопасности РФ, введенная указом Президента РФ №24 в январе 2000 г., определяет важнейшие задачи обеспечения информационной безопасности Российской Федерации:

- реализация конституционных прав и свобод граждан Российской Федерации в сфере информационной деятельности;
- совершенствование и защита отечественной информационной инфраструктуры, интеграция России в мировое информационное пространство;
- противодействие угрозе развязывания противоборства в информационной сфере.

Для обеспечения прав граждан в сфере информационных технологий и решения задач информационной безопасности, сформулированных в Концепции национальной безопасности РФ, разработаны и продолжают разрабатываться и совершенствоваться нормативные документы в сфере информационных технологий.

## 2.2. Основные положения важнейших законодательных актов РФ в области информационной безопасности и защиты информации

2.2.1. Закон Российской Федерации от 21 июля 1993 года № 5485-1 «О государственной тайне» с изменениями и дополнениями, внесенными после его принятия, регулирует отношения, возникающие в связи с отнесением сведений к государственной тайне, их рассекречиванием и защитой в интересах обеспечения безопасности Российской Федерации.

В Законе определены следующие основные понятия:

- **государственная тайна** – защищаемые государством сведения в области его военной, внешнеполитической, экономической, разведывательной, контрразведывательной и оперативно-розыскной деятельности, распространение которых может нанести ущерб безопасности Российской Федерации;
- **носители сведений, составляющих государственную тайну** – материальные объекты, в том числе физические поля, в которых сведения, составляющие государственную тайну, находят свое отображение в виде символов, образов, сигналов, технических решений и процессов;
- **система защиты государственной тайны** – совокупность органов защиты государственной тайны, используемых ими средств и методов защиты сведений, составляющих государственную тайну, и их носителей, а также мероприятий, проводимых в этих целях;
- **доступ к сведениям, составляющим государственную тайну** – санкционированное полномочным должностным лицом ознакомление конкретного лица со сведениями, составляющими государственную тайну;
- **гриф секретности** – реквизиты, свидетельствующие о степени секретности сведений, содержащихся в их носителе, проставляемые на самом носителе и (или) в сопроводительной документации на него;
- **средства защиты информации** – 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.

Законом определено, что средства защиты информации

должны иметь сертификат, удостоверяющий их соответствие требованиям по защите сведений соответствующей степени секретности.

Организация сертификации средств защиты информации возлагается на Государственную техническую комиссию при Президенте Российской Федерации, Федеральную службу безопасности Российской Федерации, Министерство обороны Российской Федерации в соответствии с функциями, возложенными на них законодательством Российской Федерации.

### 2.2.2. Закон РФ «Об информации, информатизации и защите информации» от 20 февраля 1995 года № 24-ФЗ

Данный закон является одним из основных базовых законов в области защиты информации, который регламентирует отношения, возникающие при формировании и использовании информационных ресурсов Российской Федерации на основе сбора, накопления, хранения, распространения и предоставления потребителям документированной информации, а также при создании и использовании информационных технологий, при защите информации и прав субъектов, участвующих в информационных процессах и информатизации.

Основными задачами системы защиты информации, нашедшими отражение в Законе «Об информации, информатизации и защите информации», являются:

- предотвращение утечки, хищения, утраты, несанкционированного уничтожения, искажения, модификации (подделки), несанкционированного копирования, блокирования информации и т. п., вмешательства в информацию и информационные системы;
- сохранение полноты, достоверности, целостности информации, ее массивов и программ обработки данных, установленных собственником или уполномоченным им лицом;
- сохранение возможности управления процессом обработки, пользования информацией в соответствии с условиями, установленными собственником или владельцем информации;
- обеспечение конституционных прав граждан на

сохранение личной тайны и конфиденциальности персональной информации, накапливаемой в банках данных;

- сохранение секретности или конфиденциальности информации в соответствии с правилами, установленными действующим законодательством и другими законодательными или нормативными актами;
- соблюдение прав авторов программно-информационной продукции, используемой в информационных системах.

Закон определяет:

- информационные ресурсы делятся на государственные и негосударственные (ст. 6, ч. 1).
- государственные информационные ресурсы являются открытыми и общедоступными. Исключение составляет документированная информация, отнесенная законом к категории ограниченного доступа (ст. 10, ч. 1);
- документированная информация с ограниченного доступа по условиям ее правового режима подразделяется на информацию, отнесенную к государственной тайне, и конфиденциальную (ст. 10, ч. 2).

Закон определяет пять категорий государственных информационных ресурсов:

- открытая общедоступная информация во всех областях знаний и деятельности;
- информация с ограниченным доступом:
- информация, отнесенная к государственной тайне;
- конфиденциальная информация;
- персональные данные о гражданах (относятся к категории конфиденциальной информации, но регламентируются отдельным законом).

Статья 22 Закона «Об информации, информатизации и защите информации» определяет права и обязанности субъектов в области защиты информации. В частности, пункты 2 и 5 обязывают владельца информационной системы обеспечивать необходимый уровень защиты конфиденциальной информации и оповещать собственников информационных ресурсов о фактах нарушения режима защиты информации.

Следует отметить, что процесс законотворчества идет до-

статочно сложно. Если в вопросах защиты государственной тайны создана более или менее надежная законодательная система, то в вопросах защиты служебной, коммерческой и частной информации существует достаточно много противоречий и «нестыковок».

При разработке и использовании законодательных и других правовых и нормативных документов, а также при организации защиты информации важно правильно ориентироваться во всем блоке действующей законодательной базы в этой области.

Проблемы, связанные с правильной трактовкой и применением законодательства Российской Федерации, периодически возникают в практической работе по организации защиты информации от ее утечки по техническим каналам, от несанкционированного доступа к информации и от воздействий на нее при обработке в технических средствах информатизации, а также в ходе контроля эффективности принимаемых мер защиты.

## 2.3. Ответственность за нарушения в сфере информационной безопасности

Важная роль в системе правового регулирования информационных отношении отводится ответственности субъектов за нарушения в сфере информационной безопасности.

Основными документами в этом направлении являются:

- Уголовный кодекс Российской Федерации;
- Кодекс Российской Федерации об административных правонарушениях.

В принятом в 1996 году **Уголовном кодексе Российской Федерации**, как наиболее сильнодействующем законодательном акте по предупреждению преступлений и привлечению преступников и нарушителей к уголовной ответственности, вопросам безопасности информации посвящены следующие главы и статьи:

- Статья 138. Нарушение тайны переписки, телефонных переговоров, почтовых, телеграфных или иных сообщений;
- Статья 140. Отказ в предоставлении гражданину инфор-

мации;

- Статья 183. Незаконное получение и разглашение сведений, составляющих коммерческую или банковскую тайну;
- Статья 237. Сокрытие информации об обстоятельствах, создающих опасность для жизни и здоровья людей;
- Статья 283. Разглашение государственной тайны;
- Статья 284. Утрата документов, содержащих государственную тайну.

Особое внимание уделяется компьютерным преступлениям, ответственность за которые предусмотрена в специальной 28 главе кодекса «Преступления в сфере компьютерной информации». Глава 28 включает следующие статьи:

- Статья 272. Неправомерный доступ к компьютерной информации:

1. Неправомерный доступ к охраняемой законом компьютерной информации, то есть информации на машинном носителе, в электронно-вычислительной машине (ЭВМ), системе ЭВМ или их сети, если это деяние повлекло уничтожение, блокирование, модификацию, либо копирование информации, нарушение работы ЭВМ, системы ЭВМ или их сети, – наказывается штрафом в размере от двухсот до пятисот минимальных размеров оплаты труда или в размере заработной платы или иного дохода осужденного за период от двух до пяти месяцев, либо исправительными работами на срок от шести месяцев до одного года, либо лишением свободы на срок до двух лет.

2. То же деяние, совершенное группой лиц по предварительному сговору или организованной группой, либо лицом с использованием своего служебного положения, а равно имеющим доступ к ЭВМ, системе ЭВМ или их сети, – наказывается штрафом в размере от пятисот до восьмисот минимальных размеров оплаты труда или в размере заработной платы или другого дохода осужденного за период от пяти до восьми месяцев, либо исправительными работами на срок от одного года до двух лет, либо арестом на срок от трех до шести месяцев, либо лишением свободы на срок до пяти лет.

- Статья 273. Создание, использование и распространение вредоносных программ для ЭВМ:

1. Создание программ для ЭВМ или внесение изменений в существующие программы, заведомо приводящих к несанкционированному уничтожению, блокированию, модификации либо копированию информации, нарушению работы ЭВМ, системы ЭВМ или их сети, а равно использование либо распространение таких программ или машинных носителей с такими программами, – наказывается лишением свободы на срок до трех лет со штрафом в размере от двухсот до пятисот минимальных размеров оплаты труда или в размере заработной платы или иного дохода осужденного за период от двух до пяти месяцев.

2. Те же деяния, повлекшие по неосторожности тяжкие последствия, – наказываются лишением свободы на срок от трех до семи лет.

- Статья 274. Нарушение правил эксплуатации ЭВМ, системы ЭВМ или их сети

1. Нарушение правил эксплуатации ЭВМ, системы ЭВМ или их сети лицом, имеющим доступ к ЭВМ, системе ЭВМ или их сети, повлекшее уничтожение, блокирование или модификацию охраняемой законом информации ЭВМ, если это деяние причинило существенный вред, – наказывается лишением права занимать определенные должности или заниматься определенной деятельностью на срок до пяти лет, либо обязательными работами на срок от ста восьмидесяти до двухсот сорока часов, либо ограничением свободы на срок до двух лет.

2. То же деяние, повлекшее по неосторожности тяжкие последствия, – наказывается лишением свободы на срок до четырех лет.

## 3. ПОРЯДОК ВЫПОЛНЕНИЯ РАБОТЫ

1. Изучить основные теоретические положения.

2. Оформить отчет. Отчет должен содержать: наименование и цель работы, описание основных теоретических положений, ответы на контрольные вопросы.

# 4. КОНТРОЛЬНЫЕ ВОПРОСЫ

1. Перечислите основополагающие документы по информационной безопасности.

2. Понятие государственной тайны.

3. Понятие средств защиты информации.

4. Что понимается под средствами защиты государственной тайны?

5. Основные задачи «информационной безопасности» в соответствии с Концепцией национальной безопасности РФ.

6. Какие категории государственных информационных ресурсов определены в Законе «Об информации, информатизации и защите информации»?

7. Какая ответственность в Уголовном кодексе РФ предусмотрена за создание, использование и распространение вредоносных программ для ЭВМ?

# Практическая работа №2

СИСТЕМЫ МЕНЕДЖМЕНТА КАЧЕСТВА

## 1. ЦЕЛЬ РАБОТЫ

Изучить принципы менеджмента качества, ознакомиться с современной системой менеджмента качества.

## 2. ТЕОРЕТИЧЕСКИЕ ПОЛОЖЕНИЯ

### 2.1. Понятие системы менеджмента качества

Система менеджмента качества (СМК) – это совокупность взаимосвязанных процессов, осуществляемых в организации на всех уровнях управления для достижения целей в области качества.

Система менеджмента качества (СМК) представляет собой модель менеджмента многочисленных взаимосвязанных, взаимодействующих, динамичных видов деятельности (процессов), осуществляемых организацией. Регламентирование процессов управления рекомендуется осуществлять на основе стандартов семейства ISO 9000.

ISO – аббревиатура Международной организации по стандартизации. Эта организация, наряду с нормированием требований к характеристикам продукции разрабатывает стандартизованные правила системного подхода к менеджменту.

В состав СМК входят такие процессы, как планирование целей в области качества, анализ достижений и проблем, управление персоналом и инфраструктурой, взаимодействие с потребителями, изучение их удовлетворенности, сотрудничество с поставщиками, управление проектированием и производством, контроль, мониторинг и улучшение продукции и процессов и др.

В стандарте ISO 9001:2008 «Системы менеджмента качества. Требования» установлен минимально необходимый для организации состав процессов управления качеством. Эти процессы разделены на 5 групп:

1. Процессы управления документацией СМК (разд. 4 стандарта);

2. Процессы, относящиеся к ответственности руководства (разд. 5 стандарта);

3. Процессы менеджмента ресурсов (разд. 6 стандарта);

4. Процессы в составе жизненного цикла продукции (разд. 7 стандарта);

5. Процессы измерения, анализа и улучшения качества и СМК (разд. 8 стандарта).

Процессы управления документацией имеют равное отношение ко всем группам прочих процессов СМК. Остальные группы процессов взаимосвязаны таким образом, что выходы процессов одной группы служат входами процессов другой группы, т. е. в соответствии с процессным подходом.

Связь процессов менеджмента в СМК представлена на рис. 1, который приведен в стандарте ISO 9001:2008.

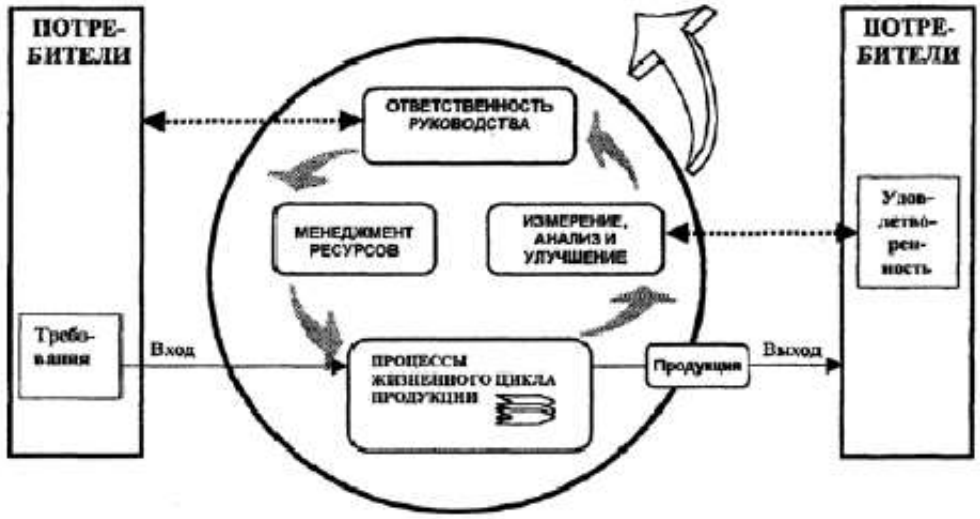


Рис. 1. Модель СМК

Все эти процессы осуществляются в любой организации. Но их взаимосвязь и взаимодействие, их направленность на удовлетворение потребителей обеспечиваются только при условии внедрения в организации стандартов семейства ISO 9000.

Приведенная на рис. 1 модель системы менеджмента качества, основанная на процессном подходе, иллюстрирует свя-

зи между процессами, представленными в разделах 4–8 стандарта. Эта модель показывает, что потребители играют существенную роль при определении входных данных. Мониторинг удовлетворенности потребителей требует оценки информации, касающейся восприятия потребителями выполнения организацией их требований. Через потребителей проходит внешний контур управления качеством: предложение на рынок продукции (услуг) – получение конкретных заказов (заявок) – изготовление и поставка продукции (услуг) потребителям – реакция потребителей на полученную продукцию и на поставляемые услуги – обработка данных об удовлетворенности и о требованиях потребителей – скорректированное предложение.

Одновременно с внешним контуром управления в СМК предусмотрен и внутренний контур: нормы и планы, поступающие от руководства – формирование ресурсной базы в соответствии с установленными внутренними нормами и планами – предоставление ресурсов в производственные подразделения – реализация продукции (от заключения контракта и проектирования до поставки и сервиса у потребителя) – получение данных о качестве продукции, процессов, ресурсов – анализ этих данных и корректировка норм и планов.

## 2.2. Принципы менеджмента качества, применяемые в стандартах ISO 9000

Для успешного руководства организацией и ее функционирования необходимо осуществлять менеджмент систематически и открыто. Рекомендации руководству организации, предлагаемые в настоящем международном стандарте, базируются на восьми принципах менеджмента качества. Эти принципы, были разработаны для применения высшим руководством с целью улучшения деятельности организации.

Они включены в содержание настоящего международного стандарта:

1. **Ориентация на потребителя**

Организации зависят от своих потребителей, и поэтому должны понимать их текущие и будущие потребности, выпол-

нять их требования и стремиться превзойти их ожидания.

2. **Лидерство руководителя**

Руководители обеспечивают единство цели и направления деятельности организации. Им следует создать и поддерживать внутреннюю среду, в которой работники могут быть полностью вовлечены в решение задач организации.

3. **Вовлечение работников**

Работники всех уровней составляют основу организации, и их полное вовлечение дает возможность организации с выгодой использовать их способности.

4. **Процессный подход**

Желаемый результат достигается эффективнее, когда деятельностью и соответствующими ресурсами управляют как процессом.

5. **Системный подход к менеджменту**

Выявление, понимание и менеджмент взаимосвязанных процессов как системы вносят вклад в результативность и эффективность организации при достижении ее целей.

6. **Постоянное улучшение**

Постоянное улучшение деятельности организации в целом следует рассматривать как ее неизменную цель.

7. **Принятие решений, основанное на фактах**

Эффективные решения основываются на анализе данных и информации.

8. **Взаимовыгодные отношения с поставщиками**

Организация и ее поставщики взаимозависимы, и отношения взаимной выгоды повышают способность обеих сторон создавать ценности.

## 2.3. Процессы общего руководства качеством в СМК

Высшее руководство организации, согласно требованиям стандарта, должно нести ответственность за следующие процессы:

– создание СМК, идентификацию процессов и связей между ними;

– формирование организационной структуры управления;

– формулировку Политики в области качества;

– планирование развития СМК;

– определение целей в области качества для организации и для всех ее уровней управления;

– назначение представителя руководства, ответственного за СМК (менеджера по качеству);

– создание и поддержание каналов обмена информацией между уровнями управления и подразделениями;

– периодический анализ проблем в области качества и прочих вопросов функционирования СМК.

Структура процессов и связи между ними могут быть представлены в виде карт процессов, где выходы предыдущих процессов используются, как входы следующих, где определены исполнители операций и виды записей, оформляемых при выполнении работ.

Организационные структуры систем управления могут быть различными. Стандарт не устанавливает требований к их конфигурации.

Различают несколько типовых организационных структур, которые делятся на две группы: иерархические и органические.

Иерархические системы управления более строго регламентированы. Обеспечивается персональная ответственность исполнителей за выполнение их функций и быстрая реакция на управленческие решения. Но усложнена связь между исполнителями по горизонтали. Система не поддается трансформации и при изменении внешних условий.

Органические системы адаптивны к внешним условиям (к изменению требований рынка и др.). Но повышается уровень требований к квалификации исполнителей. Регламентирование взаимодействий затруднено.

СМК базируется на существующей организационной структуре предприятия и использует установленные в ней взаимосвязи и каналы передачи информации.

## 2.4. Процессы ресурсного обеспечения в составе СМК

Организации для функционирования требуются ресурсы, которые подразделяют обычно на группы: человеческие, информационные, материальные, энергетические, временные, финансовые. Организация, заявляющая о своих обязательствах по производству определенных продуктов и услуг, должна определить, какие ресурсы ей нужны для создания качественной продукции.

Определив требования к ресурсам, руководство организации должно нести ответственность за приобретение и поддержание ресурсов в работоспособном состоянии.

Стандарт ISO 9001 не устанавливает требований к ресурсам.

Он определяет, какие процессы должны быть организованы для ресурсного обеспечения:

– подготовка персонала к выполнению работ, влияющих на качество продукции;

– поддержание в рабочем состоянии инфраструктуры (зданий, рабочего пространства, оборудования, инструментов);

– управление производственной средой (условиями труда, которые могут повлиять на качество продукции).

Поддержание ресурсов в требуемом состоянии представляет собой замкнутый цикл процессов, представленный на рис. 2.


Рис. 2. Цикл процессов

## 2.5. Процессы жизненного цикла продукции в составе СМК

Жизненный цикл продукции – концептуальная модель взаимозависимых видов деятельности, влияющих на качество на различных стадиях от определения потребностей до оценки их удовлетворения.

При создании и поставке продукции организация взаимодействует с потребителем (заказчиком, покупателем, клиентом) и с поставщиками (субподрядчиками), а также осуществляет внутренние процессы (проектирование, производство). Общее требование стандарта ISO 9001 в отношении всех процессов создания и поставки продукции состоит в том, что эти процессы должны быть спланированы. Должны быть определены последовательность, сроки и методы исполнения работ, чтобы у организации и у заказчика была возможность контролировать процессы и, при необходимости, корректировать их.

Процессы, связанные с потребителями, кроме поставки им продукции и услуг, имеют две задачи:

– изучение потребностей рынка и требований законодательства, и на этом основании формулирование предложений – описания продукта;

– мониторинг удовлетворенности потребителей, и на основании их отзывов корректировка предложений и конфигурации продукции.

Процессы взаимодействия с поставщиками продукции

(сырья, комплектующих изделий) и субподрядных услуг, также, предусматривают двустороннюю связь: представление поставщикам требований, получение от них продукции (услуг), оценку их качества и воздействие на поставщиков с целью улучшения качества поставляемой им продукции.

Производственные процессы, согласно требованиям стандарта, должны протекать в управляемых условиях:

1. Наличие документированных методик;

2. Использование подходящих технических средств и производственной среды;

3. Соответствие стандартам, нормам и правилам;

4. Контроль параметров процесса и управления по результатам контроля;

5. Критерии квалификации при выполнении конкретных работ (нормы качества);

6. Аттестация процессов, не поддающихся объективному текущему контролю.

Согласно Принципу процессного подхода, хозяин процесса должен знать, от кого и какие входные потоки должны быть ему обеспечены, какие должны быть созданы условия производственной среды, какими ресурсами он должен располагать, какие требования к качеству продукции на различных стадиях производства должны контролироваться.

## 2.6. Процессы постоянного улучшения

Процессы постоянного улучшения, согласно требованиям стандарта – это процессы постановки и достижения целей в области качества, корректирующие и предупреждающие действия.

Стандарт ISO 9001 рекомендует во всех процессах менеджмента применять системный подход и методологию, известную, как цикл Деминга, или цикл «Plan – Do – Check – Act» (**PDCA**):

Цикл **PDCA** можно кратко описать так:

Планирование (plan): разработка цели и процессов, необходимых для достижения результатов в соответствии с требованиями потребителей и политикой организации.

Осуществление (do): внедрение процессов.

Проверка (check): постоянный контроль и измерение процессов и продукции в сравнении с политикой, целями и требованиями на продукцию и сообщение о результатах.

Действие (act): предпринятие действий по постоянному улучшению показателей процессов.

## 2.7. Аутсорсинг в системе менеджмента качества

Аутсорсинг:

– передача стороннему подрядчику некоторых бизнес-функций или частей бизнес-процесса предприятия;

– перевод внутреннего подразделения или подразделений предприятия и всех связанных с ним активов в организацию поставщика услуг, предлагающего оказывать некую услугу в течение определенного времени по оговоренной цене;

– передача на договорной основе непрофильных функций другим организациям, которые специализируются в конкретной области и обладают соответствующим опытом, знаниями, техническими средствами;

– привлечение ресурсов специализированных организаций вместо развития собственных компетенций в конкретных видах и направлениях деятельности.

Аутсорсинг всегда связан с передачей части своей деятельности другим лицам или организациям вместо развития собственных ресурсов с целью повышения эффективности производства.

Форма партнерских взаимоотношений в рамках аутсорсинга выбирается заказчиком и зависит от желания и возможности контролировать и координировать выполнение работ.

Внедрение аутсорсинга, как комплексного решения в области результативности процессов системы менеджмента качества, организации, требует тщательной проработки и подготовки. Отдельные этапы могут иметь различную продолжительность, в зависимости от развития рынка и отрасли, актуальности проблемы делегирования процесса, стратегических и оперативных целей организации и возможности их достижения при использовании аутсорсинга. Как показывает практика,

внедрение аутсорсинга в систему менеджмента качества организации позволяет добиться постоянного улучшения ее деятельности с учетом потребностей всех заинтересованных сторон:

– организация-заказчик использует недостающие ресурсы, современные технологии, что дает возможность достичь конкурентных преимуществ;

– аутсорсер-исполнитель получает необходимые условия для развития и совершенствования основной деятельности;

– потребитель имеет возможность купить продукцию или услугу высокого качества по доступной цене.

Внедрение процесса аутсорсинга состоит из нескольких основных этапов: рассмотрение возможности передачи процессов системы менеджмента качества в аутсорсинг, поиск потенциальных аутсорсеров, разработка контракта, выполнение контракта, оценка процессов системы менеджмента качества.

## 3. ПОРЯДОК ВЫПОЛНЕНИЯ РАБОТЫ

1. Изучить основные теоретические положения.

2. Оформить отчет. Отчет должен содержать: наименование и цель работы, описание основных теоретических положений, ответы на контрольные вопросы.

## 4. КОНТРОЛЬНЫЕ ВОПРОСЫ

1. Что такое система менеджмента качества?

2. Что представляет собой ISO?

3. Каковы особенности модели СМК?

4. Каковы принципы менеджмента качества?

5. Каковы процессы общего руководства качеством в СМК?

6. Каковы процессы ресурсного обеспечения в составе СМК?

7. Что представляет собой жизненный цикл продукции в СМК?

8. Что понимается под постоянным улучшением?

9. Что представляет собой аутсорсинг СМК?

# Практическая работа №3

# СТАНДАРТЫ И СПЕЦИФИКАЦИИ В ОБЛАСТИ ЗАЩИТЫ ИНФОРМАЦИИ И ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

## 1. ЦЕЛЬ РАБОТЫ

Ознакомиться с основными стандартами и спецификациями, используемыми в сфере защиты информации и информационной безопасности.

## 2. ТЕОРЕТИЧЕСКИЕ ПОЛОЖЕНИЯ

### 2.1. Основные положения государственной информационной политики Российской Федерации

Государственная политика обеспечения информационной безопасности Российской Федерации определяет основные направления деятельности федеральных органов государственной власти и органов государственной власти субъектов Российской Федерации в этой области, порядок закрепления их обязанностей по защите интересов Российской Федерации в информационной сфере в рамках направления их деятельности и базируется на соблюдении баланса интересов личности, общества и государства в информационной сфере.

Государственная политика обеспечения информационной безопасности РФ основывается на следующих основных принципах:

– соблюдение Конституции РФ, законодательства РФ, общепризнанных принципов и норм международного права при осуществлении деятельности по обеспечению информационной безопасности РФ;

– открытость в реализации функций федеральных органов государственной власти субъектов РФ и общественных объединений, предусматривающая информирование общества об их деятельности с учетом ограничений, установленных законодательством РФ;

– правовое равенство всех участников процесса информа-

ционного взаимодействия вне зависимости от их политического, социального и экономического статуса, основывающееся на конституционном праве граждан на свободный поиск, передачу, производство и распространение информации любым законным способом;

– приоритетное развитие отечественных современных информационных и телекоммуникационных технологий, производство технических и программных средств, способных обеспечить совершенствование национальных телекоммуникационных сетей, их подключение к глобальным информационным сетям в целях соблюдения жизненно важных интересов РФ.

Государство в процессе реализации своих функций по обеспечению информационной безопасности РФ:

– проводит объективный и всесторонний анализ и прогнозирование угроз информационной безопасности РФ, разрабатывает меры по ее обеспечению;

– организует работу законодательных и исполнительных органов государственной власти РФ по реализации комплекса мер, направленных на предотвращение, отражение и нейтрализацию угроз информационной безопасности РФ;

– поддерживает деятельность общественных объединений, направленную на объективное информирование населения о социально значимых явлениях общественной жизни, защиту общества от искажений и недостоверной информации;

– осуществляет контроль над разработкой, созданием, развитием, использованием, экспортом и импортом средств защиты информации посредством их сертификации и лицензирования деятельности в области защиты информации;

– проводит необходимую протекционистскую политику в отношении производителей средств информатизации и защиты информации на территории РФ и принимает меры по защите внутреннего рынка от проникновения на него некачественных средств информатизации и информационных продуктов;

– способствует предоставлению физическим и юридическим лицам доступа к мировым информационным ресурсам, глобальным информационным сетям;

– формулирует и реализует государственную информационную политику России;

– организует разработку федеральной программы обеспечения информационной безопасности РФ;

– способствует интернационализации глобальных информационных сетей и систем, а также вхождению России в мировое информационное сообщество на условиях равноправного партнерства.

Совершенствование правовых механизмов регулирования общественных отношений, возникающих в информационной сфере, является приоритетным направлением государственной политики в области обеспечения информационной безопасности РФ.

Это предполагает:

– оценку эффективности применения действующих законодательных и иных нормативных правовых актов в информационной сфере и выработку программы их совершенствования;

– создание организационно-правовых механизмов обеспечения информационной безопасности;

– определение правового статуса всех субъектов отношений в информационной сфере, включая пользователей информационных и телекоммуникационных систем, и установление их ответственности за соблюдение законодательства РФ в данной сфере;

– создание системы сбора и анализа данных об источниках угроз информационной безопасности РФ, а также о последствиях их осуществления;

– разработку нормативных правовых актов, определяющих организацию следствия и процедуру судебного разбирательства по фактам противоправных действий в информационной сфере, а также порядок ликвидации последствий этих противоправных действий;

– разработку составов правонарушений с учетом специфики уголовной, гражданской, административной, дисциплинарной ответственности и включение соответствующих правовых норм в уголовный, гражданский, административный и трудовой кодексы, в законодательство РФ о государственной службе;

– совершенствование подготовки кадров, используемых в области обеспечения информационной безопасности РФ.

Правовое обеспечение информационной безопасности РФ должно базироваться, прежде всего, на соблюдении принципов законности, баланса интересов граждан, общества и государства в информационной сфере.

Соблюдение принципа баланса интересов граждан, общества и государства в информационной сфере предполагает законодательное закрепление приоритета этих интересов в различных областях жизнедеятельности общества.

## 2.2. Первоочередные мероприятия по реализации государственной политики обеспечения информационной безопасности

Первоочередными мероприятиями по реализации государственной политики обеспечения информационной безопасности РФ являются:

– разработка и внедрение механизмов реализации правовых норм, регулирующих отношения в информационной сфере, а также подготовка концепции правового обеспечения информационной безопасности РФ;

– разработка и реализация механизмов повышения эффективности государственного руководства деятельностью государственных средств массовой информации, осуществление государственной информационной политики;

– принятие и реализация федеральных программ, предусматривающих формирование общедоступных архивов информационных ресурсов, повышение правовой культуры и компьютерной грамотности граждан, развитие единого информационного пространства России, комплексное противодействие угрозам информационной войны, создание безопасных информационных технологий, пресечение компьютерной преступности, обеспечение технологической независимости страны в области создания информационных систем;

– развитие системы подготовки кадров, используемых в области обеспечения информационной безопасности Российской Федерации.

### 2.2.1. Оценочные стандарты и технические спецификации. «Оранжевая книга» как оценочный стандарт. Основные понятия

Существует два вида стандартов и спецификаций:

– оценочные стандарты, направленные на классификацию информационных систем и средств защиты по требованиям безопасности;

– технические спецификации, регламентирующие различные аспекты реализации средств защиты.

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.

Степень доверия оценивается по двум основным критериям.

**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.

**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.

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.

**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 по-

вторного 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.

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, 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 убе-

диться 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».

## 2.3. Информационная безопасность распределенных систем. Рекомендации X.800. Сетевые сервисы безопасности

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 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 неотка-

зуемости является **аутентификация источника данных.**

2.3.1. 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.

### 2.3.2. Администрирование средств безопасности

Оно 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.

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).

Таким образом, администрирование средств безопасности в распределенной ИС имеет особенности по сравнению с централизованными системами.

### 2.3.3. Стандарт ISO/IEC 15408 «Критерии оценки безопасности информационных технологий». Основные понятия

По историческим причинам данный стандарт часто называют «Общими критериями» (ОК).

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. 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 реализую-

щим 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.

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.** 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.

**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.

**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, что значительно больше, чем число аналогичных сущностей в «Оранжевой книге».

Существуют следующие классы функциональных требо-

ваний 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).

## 3. ПОРЯДОК ВЫПОЛНЕНИЯ РАБОТЫ

1. Изучить основные теоретические положения.

2. Оформить отчет. Отчет должен содержать: наименование и цель работы, описание основных теоретических положений, ответы на контрольные вопросы.

## 4. КОНТРОЛЬНЫЕ ВОПРОСЫ

1. Каковы принципы государственной политики РФ в области информационной безопасности?

2. Какие действия проводит государство в процессе реализации своих функций по обеспечению информационной безопасности РФ?

3. Каковы первоочередные мероприятия по реализации

государственной политики обеспечения информационной безопасности РФ?

4. Что понимается под политикой безопасности?

5. Какие элементы включает в себя политика безопасности?

6. Что включает в себя операционная гарантированность?

7. Какие механизмы используются для реализации сервисов (функций) безопасности?

8. Что такое функциональный пакет?

9. Какие существуют классы функциональных требований общих критериев?

## Практическая работа №4

# ОСНОВНЫЕ ВИДЫ ТЕХНИЧЕСКОЙ И ТЕХНОЛОГИЧЕСКОЙ ДОКУМЕНТАЦИИ

## 1. ЦЕЛЬ РАБОТЫ

Ознакомиться с нормативно-правовыми основами «информационной безопасности» в РФ, нормативными документами и ответственностью за нарушения информационной безопасности.

## 2. ТЕОРЕТИЧЕСКИЕ ПОЛОЖЕНИЯ

### 2.1. Нормативно-методическая база документоведения и основные понятия о документе и сообщении

В процессе решения большинства задач возникает потребность в каких-либо сведениях. Эти сведения, т. е. информацию, получают в готовом виде из определенных источников (документов), в которых эти сведения могут находиться. Классификация информации (рис. 1) предусматривает два вида информации: *документальную*, т. е. сведения об источниках, где могут находиться необходимые данные и *фактографическую*, то есть собственно данные, пригодные для использования.

Исходя из этого, документоведение – это научная дисциплина, изучающая в историческом развитии закономерности образования документов, способы их создания, становления и развития систем документации и систем документоведения. Важнейшей задачей документоведения является теоретическое обоснование процессов документационного обеспечения аппарата управления обществом.

Нормативно-методическую базу документоведения в Российской Федерации составляют:

– законодательные акты Российской Федерации в сфере информации и документации;

– указы и распоряжения Президента РФ, постановления и распоряжения правительства РФ, регламентирующие вопро-

сы документационного обеспечения на федеральном уровне;

– правовые акты федеральных органов исполнительной власти (министерств, агентств и др.) как общеотраслевого, так и ведомственного характера;

– правовые акты органов власти субъектов Российской Федерации и их территориальных образований;

– правовые акты нормативного и инструктивного характера, методические документы организаций и предприятий;

– государственные стандарты на документацию;

– унифицированные системы документации;

– общероссийские классификаторы технико-экономической и социальной информации;

– государственная система документационного обеспечения управления;

– нормативные документы по организации управленческого труда и охране труда;

– нормативные документы по организации архивного хранения документов.


Рис. 1. Классификация информации

*Документ* – это зафиксированная на материальном носителе информация с реквизитами, позволяющими ее идентифицировать. Под *реквизитом* понимается обязательный элемент оформления официального документа.

Для передачи и хранения информации используются различные знаки (символы), позволяющие представить ее в определенной форме. Этими символами могут быть слова и фразы человеческой речи, тексты, рисунки, математические знаки, формы колебаний и т. п. Совокупность знаков, отображающих ту или иную информацию, называется *сообщением*.

Так, например, при телеграфной передаче сообщением является текст телеграммы, представляющий собой последовательность отдельных знаков — букв и цифр. При разговоре по телефону сообщением выступает изменение во времени звукового давления, отображающее не только содержание, но и интонацию, тембр, ритм и другие свойства речи. При передаче движущихся изображений в телевизионных системах сообщение представляет собой изменение во времени яркости элементов изображения.

Таким образом, сообщение – это кодированный эквивалент события, зафиксированный источником информации и выраженный с помощью последовательности условных физических символов, образующих некоторую упорядоченную совокупность. Переменные, функцией которых является сообщение, могут быть заданы следующим перечнем:

– целевая направленность сведений, отраженных в сообщении, определяющая область их применения;

– содержание сообщения, т. е. данные, отражаемые в сообщении и определяющие его практическую ценность;

– языки (алфавиты, правила, методы, алгоритмы, программы) преобразования информации (сведений и соответствующих им сообщений), в том числе при изменении носителя информации, устройств воспроизведения, фиксации, сбора, передачи, хранения, обработки, ввода-вывода сообщений;

– устройства, обеспечивающие взаимодействие источника и приемника при передаче-приеме сообщений, а также их обработку;

– способ сохранения (закрепления, записи) информации;

– носитель информации.

В основном используют следующие виды носителей: бумажные (для традиционных видов полиграфии); магнитные и магнитооптические (магнитные ленты, диски и др.); микро-

фильмовые и кинофотоматериалы; устройства отображения (табло для алфавитно-цифровой информации, экраны, самолинзы).

## 2.2. Отличительные свойства, признаки и конфиденциальность документа

Документ как частный случай сообщения обладает всеми инвариантными свойствами информации, но в отличие от сообщения он имеет ряд свойств (функций и признаков), налагаемых на него сектором действенности в целях его последующего общественного использования.

Отсюда вытекают следующие свойства, которыми должно обладать сообщение, чтобы стать документом: *доступность*, *подлинность* и *легитимность*.

Одним из основополагающих понятий в документоведении является качество документа, под которым понимается совокупность присущих документу существенных признаков и особенностей, позволяющих выделить его из среды других предметов.

*Признак документа* – это показатель (параметр, атрибут), по которому можно определить тот или иной предмет как документ. Признаки документа подразделяют на внешние и внутренние.

Внешние признаки отображают форму и размер документа, носитель информации, способ записи, элементы оформления (реквизиты).

К внутренним признакам документа относятся его язык, стиль, юридическая и управляющая силы.

Конкретный набор реквизитов для каждого документа определяется его разновидностью. Однако существует группа элементов, присущих любому документу, поскольку они характеризуют его юридическую силу, т. е. позволяют его идентифицировать именно как документ, а не как сообщение. К их числу относятся: авторство, наименование вида документа, датирование, удостоверение, которые в совокупности с формой и размером документа, способом документирования и используемым носителем информации составляют документообразующие признаки.

*Вид документа* – это классификационное понятие, употребляемое для обозначения группы документов одного наименования, имеющих общее назначение и единую структуру построения. Например, протоколы это один вид, приказы – другой, отчеты – третий и т. д.

*Разновидность документа* – более узкое, частное понятие, которое детализирует, уточняет характер деятельности, документируемой тем или иным видом. Например, акт экспертизы, акт приемки, акт инвентаризации и т. д.

Для обретения документом своего основного свойства – юридической и управленческой силы – он должен отвечать следующим требованиям:

– документ не должен противоречить действующему законодательству, нормативным и правовым актам, а также руководящим документам вышестоящих органов;

– орган, издавший данный документ, должен обладать соответствующей компетенцией, определяемой ему нормативно-правовыми актами;

– документ должен быть изготовлен и оформлен по определенной технологии.

Согласно Федеральному закону от 27 июля 2006 г. № 149-ФЗ «Об информации, информационных технологиях и защите информации» информация может являться объектом публичных, гражданских и иных правовых отношений. Информация в зависимости от категории доступа к ней подразделяется на *общедоступную* и *конфиденциальную*, т. е. информацию, доступ к которой ограничен федеральными законами и другими официальными документами.

Информация в зависимости от порядка ее представления или распространения подразделяется на следующие категории:

– свободно распространяемая;

– предоставляемая по соглашению лиц, участвующих в соответствующих отношениях;

– подлежащая предоставлению или распространению в соответствии с федеральными законами;

– распространение которой ограничено или запрещено в Российской Федерации.

В целях защиты основ конституционного строя, нравственности, здоровья, прав и законных интересов граждан и других субъектов социума, обеспечения обороны страны и безопасности государства федеральными законами устанавливается ограничение доступа к информации. При этом действуют следующие общие правила:

1. Обязательным является соблюдение конфиденциальности информации, доступ к которой ограничен федеральными законами.

2. Защита информации, составляющей государственную тайну, осуществляется в соответствии с законодательством Российской Федерации о государственной тайне.

3. Информация, составляющая коммерческую, служебную или иную тайны, подлежит защите.

4. Информация, полученная гражданами при исполнении ими профессиональных обязанностей или организациями при осуществлении ими определенных видов деятельности, также подлежит защите.

5. Информация, составляющая профессиональную тайну, может быть предоставлена третьим лицам только в соответствии с федеральными законами или по решению суда.

6. Запрещается требовать от гражданина предоставление информации, касающейся его частной жизни, в том числе информации, составляющей его личную или семейную тайну

## 2.3. Способы и средства документирования. Классификация носителей информации

В документоведении для определения процесса фиксирования информации посредством создания документа введено понятие «документирование».

*Документирование* – это запись информации на различных носителях по установленным правилам. Различают следующие способы документирования:

Текстовое документирование – наиболее древний способ фиксирования информации. Его становление и развитие неразрывно связано с возникновением письменности. С изобретением пишущей машинки появилась машинопись как метод тек-

стового документирования. Машинопись быстро вытеснила ручные способы при окончательном оформлении и копировании документа.

Однако и в настоящее время ручное текстовое документирование остается распространенным способом первоначального составления документа.

Техническое документирование является способом запечатления технической мысли. Технические документы – это обобщающее название документов, отражающих результаты строительного и технологического проектирования, конструирования, инженерных разработок и других работ по строительству зданий и сооружений и изготовлению изделий промышленного производства.

В соответствии с производственным назначением технические документальные материалы классифицируются на группы, отражающие описание:

– средств производства – конструкторская документация;

– зданий и сооружений – проектно-сметная документация;

– процессов труда – технологическая документация;

– результатов научных исследований – научно-техническая документация;

– явлений и процессов природы – документация, связанная с геодезией, картографией, гидрометеослужбой и др.;

– процессов, возникающих в сфере обращения и обслуживания.

В состав указанных групп могут входить различные графические и текстовые документы: чертежи, расчеты, технические описания, графики, технологические карты, проектные документы, картографические материалы и др.

Средства документирования можно подразделить на простые и сложные. К *простым* средствам документирования относятся так называемые рукописные средства (карандаши, ручки и др.), которые в своем развитии прошли путь от резца первобытного художника и гусиного пера до фломастеров и современных перографов (самописцев).

В настоящее время создаются и совершенствуются механические и электромеханические средства (пишущие машинки, магнитофоны, диктофоны, фото-, кино-, видеотехника и др.).

Широкое распространение получило документирование на основе компьютерной оргтехники (принтеры, плоттеры, программные продукты для персональных компьютеров), а также средства передачи и приема информации: телетайпы, факсимильные аппараты, передающие и принимающие текстовую и графическую информацию.

К *сложным* средствам документирования относятся средства репрографии и оперативной полиграфии, т.е. совокупности машин, предназначенных для копирования и тиражирования документов.

Средствами репрографии (копирования) являются средства фотокопирования, электрофотографии, термографии, электронно-лучевого копирования, микрофильмирования и ризографического копирования.

В документоведении под *носителем документированной информации* понимается материальный объект, используемый для закрепления и хранения на нем речевой, звуковой или изобразительной информации, в том числе в преобразованном виде. Таким образом, носитель информации – это физический или материальный объект, в том числе физическое поле, в котором информация находит свое отображение в виде символов, образов, сигналов, технических решений и процессов.

Наибольшую популярность до сих пор сохраняют дисковые накопители. Выделяют гибкие и жесткие, сменные и несменные магнитные, магнитооптические и оптические диски и дискеты.

Магнитный диск (дискета) – это носитель информации в виде алюминиевого или пластмассового диска, покрытого магнитным слоем. Жесткие магнитные диски предназначены для накопления и постоянного хранения информации, часто используемой в работе. Они представляют собой пакет жестко скрепленных между собой нескольких алюминиевых дисков, размещенных в герметичном корпусе.

Первыми из оптических накопителей появились компактные лазерные диски. Стандартная емкость такого компактного диска (CD) диаметром 120 мм составляет 700 Мбайт (80 мин). CD- накопители подразделяются на диски:

– только для чтения (англ. Compact Disk – Read Only

Memory – CD-ROM) с предварительно (заводским методом) записаннойна него информацией;

– для однократной записи (англ. Compact Disk Recordable– CD-R);

– многократной перезаписи (англ. Compact Disk ReWritable – CD-RW).

Цифровой универсальный диск (англ. Digital Versatile Disc – DVD) применяется для накопления видеоизображений и больших объемов любой компьютерной информации.

К твердотельным накопителям относятся голографические накопители, флэш-память и др. Технология флэш-памяти появилась в 1988 г. Носитель информации (накопитель) представляет собой микросхему с электронной энергонезависимой памятью, способную хранить записанную информацию в течение неограниченного времени и сохранять свое состояние до подачи на выводы электрического сигнала иной полярности.

## 2.4. Типы документов и требования к их составлению

По происхождению различают документы: личные и официальные. *Личные* сообщения, например, личная переписка, дневники, воспоминания личного характера, создаются вне сферы служебной деятельности человека и официальными документами не являются.

*Официальный* документ создается юридическим или физическим лицом с обязательным оформлением и удостоверением в установленном порядке. Делопроизводственные службы, как правило, работают только с официальными документами. Среди официальных документов выделяют группу личных: удостоверяющих личность (паспорт), специальность, образование (диплом, аттестат), трудовой стаж (трудовая книжка) и т. д.

*По способу документирования* различают документы: рукописные – текстовые, графические; фотодокументы; фонодокументы; кинодокументы; видеодокументы; документы, созданные с помощью компьютерной техники.

*По месту составления* документы подразделяют на входящие (поступающие); исходящие (отправляемые из организации); внутренние (создаваемые и используемые для обеспече-

ния внутренних связей данной организации).

*По форме представления* документы делят на подлинники (оригиналы), копии и дубликаты.

Подлинник (оригинал) – это первый (или единичный) экземпляр официального документа, обладающий юридической силой.

Копия документа может быть факсимильной или свободной. Копии могут воспроизводить часть текста документа (выписки) или весь документ. *Факсимильная копия* полностью воспроизводит содержание документа и все его внешние признаки – содержащиеся в подлиннике реквизиты (включая подпись и печать).

Факсимильная копия изготовляется на копировальной технике с использованием фотографии и аппарата факсимильной связи.

*Свободная копия* создается на пишущих машинках, содержит все реквизиты документа, но не обязательно повторяет его форму.

Копии, заверенные в установленном порядке, имеют такую же юридическую силу, как и подлинники. Копии, заверенные нотариусом, называются *нотариальными*.

*Дубликат* – это копия официального документа, имеющая юридическую силу подлинника и сопровождаемая отметкой «Дубликат». Дубликат выдают взамен утраченного подлинного документа (диплома, аттестата, паспорта).

По степени подлинности документы могут быть *подлинными* и *подложными* (фальсифицированными).

Документ, в котором содержатся признаки, свидетельствующие о его подлинности (например, сведения об авторе, времени и месте создания, наличие подписи автора и заверение ее оттиском печати), считается подлинным. Однако эти признаки являются и основными объектами фальсификации.

*Подложные* (фальсифицированные) документы появились, как только документ стал использоваться для доказательства тех или иных фактов. Например, фальшивые расписки, подложные завещания и др.

Наиболее часто встречаются следующие способы подделки документов: подлог – замена одного документа другим; ин-

терполяция – подложная вставка в текст подлинного документа; подделка отдельных слов и реквизитов (подписей, дат, оттисков печатей и т. д.).

В зависимости от сферы деятельности выделяют следующие виды официальных документов: управленческие и технические.

*Управленческие* документы подразделяют на организационные, распорядительные и информационно-справочные. *Организационные* документы служат правовой основой деятельности организации. *Распорядительные* документы предназначены для регулирования деятельности организации. Информация о фактическом положении дел в системе управления содержится в различных источниках, но важнейшее место среди них занимают *информационно-справочные* документы.

*Техническая документация* – это система текстовых и графических документов, содержащих информацию о технических изделиях, технических и технологических процессах и т. д. Наиболее широко используются следующие виды технической документации:

– научно-исследовательская, которая создается в процессе проведения научных исследований в различных отраслях науки и техники, а также выполнения теоретических и прикладных научно-технических разработок;

– конструкторская – включает в себя графические и текстовые документы, которые в отдельности или в совокупности определяют состав и устройство изделия и содержат необходимые данные для его разработки, изготовления, контроля, приемки, эксплуатации и ремонта;

– технологическая – совокупность графических и текстовых технических документов, которые отдельно или в комплексе определяют процесс изготовления изделий промышленного производства или процесс сооружения объектов капитального строительства;

– проектно-сметная – создается при решении вопросов о возведении, реконструкции и ремонте объектов капитального строительства.

Требования к составлению и оформлению управленческих документов закрепляются в государственных стандартах. Сре-

ди систем управленческой документации, используемых для документирования различных управленческих действий, особое значение имеет система организационно-распорядительной документации.

Документы, входящие в эту систему, применяются в учреждениях и организациях всех уровней управления, направлений деятельности и форм собственности.

Требования к составлению и оформлению технической документации определены соответствующими стандартами. Например, конструкторская документация регламентируется стандартами *Единой системы конструкторской документации* (ЕСКД), технологическая документация – стандартами *Единой системы технологической документации* (ЕСТД).

ЕСКД – это комплекс стандартов, устанавливающих взаимосвязанные нормы и правила по разработке, оформлению и обращению конструкторской документации, разрабатываемой и применяемой на всех стадиях жизненного цикла изделия (проектирования, изготовления, эксплуатации, ремонта и т. д.). Основное назначение стандартов ЕСКД состоит в установлении единых оптимальных правил выполнения, оформления и обращения конструкторской документации.

Стандарты ЕСКД распространяются на изделия машино- и приборостроения. Установленные стандартами ЕСКД нормы

и правила распространяются на следующую документацию:

– все виды конструкторских документов;

– учетно-регистрационная документация для конструкторских документов;

– документация по внесению изменений в конструкторские документы;

– нормативно-техническая, технологическая, программная документация, а также научно-техническая и учебная литература в той части, в которой они могут быть для них применимы и не регламентируются другими стандартами и нормативами, например, форматы и шрифты для печатных изданий и т.п.

Установленные в стандартах ЕСКД нормы и правила распространяются на указанную документацию, разработанную предприятиями и предпринимателями (субъектами хозяйствен-

ной деятельности), в том числе научно-техническими, инженерными обществами и другими общественными объединениями.

## 2.5. Классификация документов и системы документации

Классификация документов. В документоведении используется следующее определение: «Классификация – это разделение множества объектов на подмножества по их сходству или различию в соответствии с принятыми методами».

Так как функционирование аппарата управления невозможно без документооборота и организованной работы с документами, то классификация документов является не только научной, но и важнейшей прикладной задачей. Кроме того, классификация представляет собой также средство построения систем хранения и поиска информации.

При построении систем классификации документов используются следующие термины и определения.

*Признак классификации* – признак, по которому осуществляется деление данного множества на подмножества.

*Значение признака классификации* – конкретное количественное или качественное выражение признака классификации.

*Классификационная группировка* – подмножество, полученное в результате разделения заданного множества по одному или нескольким признакам классификации.

*Кодовый алфавит* – конечное множество кодовых знаков, из которых по определенным правилам составляются кодовые обозначения.

*Код* – совокупность кодовых обозначений.

*Кодовое обозначение* – обозначение объекта классификации (признака, значения признака, классификационной группировки) знаком или группой знаков в соответствии с принятым методом кодирования.

*Метод (правило) кодирования* – метод образования и присвоения кодового обозначения объекту классификации, а также признаку, значению признака, классификационной группировке.

*Структура кодового обозначения* – порядок расположе-

ния знаков в кодовом обозначении.

*Длина кодового обозначения* – количество знаков в кодовом обозначении.

*Классификатор, классификационная схема* – систематизированный перечень наименований объектов классификации, признаков, значений признаков, классификационных группировок и их кодовых обозначений.

**Системы классификации и кодирования документации**. В условиях автоматизации процессов управления и применения современных информационных технологий единицей хранения, обработки, информационного обмена и поиска является не только документ в целом, но и его элементы: реквизиты и отдельные элементы его содержания. Таким образом, возникла потребность в классификации этих отдельных элементов как самостоятельных объектов.

Для автоматизации обработки не только основных информационных сообщений и документов, но и всех видов информации, используемой в управлении, разработан специальный инструмент классификации – стандартный язык формализованного описания данных. Была разработана Единая система классификации и кодирования технико-экономической и социальной информации. Эта система состоит из общероссийских классификаторов технико-экономической и социальной информации, средств их ведения, а также нормативных и методических документов по их разработке и применению.

В частности, в Общероссийском классификаторе информации об общероссийских классификаторах закреплена общая классификация классификаторов технико-экономической и социальной информации, в соответствии с которой все общероссийские классификаторы распределены на следующие группы в зависимости от вида информации, для которой они предназначены:

– социальная информация;

– информация по организации экономики;

– информация о продукции, видах экономической деятельности и оказываемых услугах;

– информация о природных и трудовых ресурсах;

– информация о финансово-кредитной сфере;

– информация об управленческой документации, показателях и единицах измерения;

– информация о стандартах и технологических процессах;

– прочие виды технико-экономической и социальной информации.

Общероссийские классификаторы разрабатываются для обеспечения:

– сопоставимости данных в различных областях и уровнях хозяйственной деятельности;

– совместимости с международными классификаторами;

– информационной связи с действующими общероссийскими классификаторами;

– использования их в общероссийских унифицированных формах документов.

Общероссийские классификаторы технико-экономической и социальной информации относятся к нормативным документам и по своему статусу соответствуют государственным (федеральным) стандартам Российской Федерации.

**Унифицированные системы документации**. Классификаторы технико-экономической и социальной информации, кроме реализации универсального формализованного языка описания данных, в информационном обеспечении управления выполняют еще ряд важных функций. Большой объем информации, заложенной в классификаторах, является основой для создания различными ведомствами своих реестров и регистров справочно-информационных массивов. Классификаторы технико-экономической и социальной информации также являются базой для осуществления как формальной, так и содержательной унификации документов управления.

Большое значение имеет Общероссийский классификатор управленческой документации, который представляет собой номенклатуру унифицированных систем документации и форм документов. Он содержит наименование видов документов и их коды, которые являются идентификаторами форм документов и в обязательном порядке указываются на бланках.

*Система документации* – это совокупность документов, взаимосвязанных по признакам: происхождения, назначения, вида, сферы деятельности (применения), единых требований

к их оформлению.

В делопроизводстве различных организаций соотношение документов из различных систем документации является неодинаковым, так как это зависит от направлений деятельности конкретной организации. Однако в деятельности любой организации используются документы, регламентирующие исполнительскую, распорядительную и организационную деятельность, которые унифицированы.

Унифицированная система документации – это система документации, созданная по единым правилам и требованиям, содержащая информацию, необходимую для управления в определенной сфере деятельности. Применение унифицированных форм в практике управления позволяет получить значительный экономический эффект за счет снижения затрат на составление и оформление документов, их передачу и обработку; ускорения прохождения документов; оптимизации документооборота.

В состав унифицированной системы документации входят системы:

– банковской документации;

– финансовой, учетной и отчетной бухгалтерской документации;

– отчетно-статистической документации;

– документации по труду;

– документации Пенсионного фонда Российской Федерации;

– внешнеторговой документации;

– организационно распорядительной документации.

## 3. ПОРЯДОК ВЫПОЛНЕНИЯ РАБОТЫ

1. Изучить основные теоретические положения.

2. Оформить отчет. Отчет должен содержать: наименование и цель работы, описание основных теоретических положений, ответы на контрольные вопросы.

# 4. КОНТРОЛЬНЫЕ ВОПРОСЫ

1. Что такое документоведение?
2. Что составляет нормативно-методическую базу документоведения в Российской Федерации?
3. Что такое признак документа, вид документа, разновидность документа?
4. Какими основными требованиями должен отвечать документ?
5. Каковы основные правила ограничения доступа к информации?
6. Что называется носителем документированной информации?
7. Каковы основные виды технической документации?
8. Что такое ЕСКД?
9. Что такое система документации?