ГОСУДАРСТВЕННОЕ БЮДЖЕТНОЕ ПРОФЕССИОНАЛЬНОЕ ОБРАЗОВАТЕЛЬНОЕ УЧРЕЖДЕНИЕ ИРКУТСКОЙ ОБЛАСТИ «ЧЕРЕМХОВСКИЙ ГОРНОТЕХНИЧЕСКИЙ КОЛЛЕДЖ ИМ. М.И. ЩАДОВА»

РАССМОТРЕНО
на заседании ЦК
«Информатики и ВТ»
Протокол №10
«06» июнь 2023 г.
Председатель: Чипиштанова Д.В.

УТВЕРЖДАЮ
Зам. директора по УР
О.В. Папанова
«07» июнь 2023 г.

МЕТОДИЧЕСКИЕ УКАЗАНИЯ

для выполнения
практических (лабораторных) занятий студентов
по учебной дисциплине (профессиональному модулю)

ОП. 09 СТАНДАРТИЗАЦИИ, СЕРТИФИКАЦИИ И ТЕХНИЧЕСКОЕ ДОКУМЕНТОВЕДЕНИЕ

программы подготовки специалистов среднего звена

09.02.07 «Информационные системы и программирование»

Разработал преподаватель:
О.В. Папанова

2023 г.

СОДЕРЖАНИЕ

1. ПОЯСНИТЕЛЬНАЯ ЗАПИСКА.

Методические указания по выполнению практических (лабораторных) работ по учебной дисциплине **«Стандартизация, сертификация и техническое документоведение»** предназначены для студентов специальности **09.02.07 Информационные системы и программирование**, составлены в соответствии с рабочей программой дисциплины «Метрология, стандартизация, сертификация и техническое документоведение» и направлены на достижение следующих целей:

- приобретение навыков работы со стандартами и умения анализировать их содержание;
- ознакомление с основными нормами взаимозаменяемости продукции и стандартизацией точности ГЦС;
- научиться переводить неметрические единицы измерения в единицы СИ,
- выбирать средства измерений и измерять ими линейные размеры.

Методические указания являются частью учебно-методического комплекса по дисциплине **«Стандартизация, сертификация и техническое документоведение».** Методические указания включает:

- задания к темам занятий с указанием порядка их выполнения;
- приложения рекомендаций и методических указаний по стандартизации, бланки документов, которые являются частью материального обеспечения занятий.

В качестве приложения к методическим указаниям являются:

1. Закон РФ «Об обеспечении единства измерений»;
2. Федеральный закон «О техническом регулировании»;
3. Стандарты НСС: ГОСТ Р 1.0-2004, ГОСТ Р 1.12-2004, ГОСТ Р 1.2-2004, ГОСТ Р 1.4-2004, ГОСТ Р 1.5-2004, ГОСТ Р 1.9-2004, ГОСТ 2.114-95.
4. Система сертификации ГОСТ Р
5. Фрагменты стандартов ЕСДП.
6. Ответы к заданиям с решением.

Перед каждым практическим занятием студент должен подготовить соответствующий теоретический материал по лекционным записям, на практическом занятии пополнить его по пособию, ознакомиться с заданием, материалами для выполнения работы. Ориентируясь на порядок выполнения задания, приступить к выполнению практической работы.

Для совершенствования теоретических и практических знаний, каждая Практическое занятие содержит контрольные вопросы и список литературы. Студент отвечает на контрольные вопросы при защите практической работы.

В результате выполнения полного объема практических работ студент 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.

При проведении практических работ применяются следующие технологии и методы обучения:

В соответствии с учебным планом программы подготовки специалистов среднего звена по специальности **09.02.07 Информационные системы и программирование** и рабочей программой на практические (лабораторные) работы по дисциплине **«Стандартизация, сертификация и техническое документоведение»** отводится 14 часов

2. ПЕРЕЧЕНЬ ПРАКТИЧЕСКИХ РАБОТ

№ п/п	Название практической работы	Количество часов
1	Нормативно-правовые документы и стандарты в области защиты информации и информационной безопасности	2
2	Стандарты и спецификации в области информационной безопасности Российское и зарубежное законодательство в области ИБ. Обзор международных и национальных стандартов и спецификаций в области ИБ: «Оранжевая книга», ИСО 15408 и др.	2
3	Системы менеджмента качества	2
4	Составление схемы этапов сертификации и их составляющих. Отработка правил составления сертификата	2
5	Выборка и составление схемы сертификации для специальности информационные системы	2
6	Основные виды технической и технологической документации	2
7	ЕСКД. ГОСТ 2.101-93. ГОСТ 2.104-68 ЕСКД Основные надписи. Оформление основной надписи, рамок, колонтитулов. Оформление спецификации сборочного чертежа согласно ГОСТ 2. 108-68	2
	Итого	**14**

3. СОДЕРЖАНИЕ ПРАКТИЧЕСКИХ РАБОТ.

Практическое занятие № 1

Нормативно-правовые документы и стандарты в области защиты информации и информационной безопасности

Цель занятия: Познакомить обучающихся с видами сертификации качества товаров, с порядком проведения сертификации качества в РФ.

Порядок проведения занятия: Используя теоретическое обоснование в полном объеме выполнить практические задания.

Теоретическое обоснование

Сертификат соответствия – документ, удостоверяющий соответствие объекта требованиям технических регламентов, положениям стандартов и условиям договоров. Различают обязательную сертификацию и добровольную.

Обязательная сертификация – это форма контроля со стороны государства за безопасность продукции. Ее существование связано с определенными обязанностями, налагаемыми на предприятия.

Добровольная сертификация проводится в соответствии с федеральным законом «О техническом регулировании» по инициативе заявителей (изготовителей, продавцов, исполнителей) в целях подтверждения соответствия продукции (услуг) требованиям стандартов, технических условий и других документов, определенных заявителем.

Добровольная сертификация проводится на условиях договора между заявителем и органом по сертификации.

Порядок сертификации.

Сертификация проходит по следующим основным этапам:

1. Рассмотрение и принятие решения по заявке. Органы по сертификации (ОС) рассматривает заявку и не позднее в срок - 15 дней сообщает заявителю решение.
2. Отбор, идентификация образцов и их испытания. Отбор образцов для испытания осуществляет как правило ИЛ (Испытательные Лаборатории).

3. Проверка производства (анализ состояния производства, сертификация производства и системы качества).

4. Анализ получения результатов, принятие решения о возможности выдачи сертификата.

В случае положительных результатах – ОС оформляет сертификат и регистрирует его. При отрицательных результатах обязательной сертификации выпускаемой продукции (товара, услуги) – ОС территориальный орган государственного контроля и надреза по месту расположения изготовителя (продавца, исполнителя работ) для принятия необходимых мер по предупреждению реализации данной продукции или выполнения работ. Срок действия сертификата устанавливает ОС, но не более чем на 3 года

Общие выводы по занятию:

_____

_____

_____

Практическое занятие № 2

Стандарты и спецификации в области информационной безопасности
Российское и зарубежное законодательство в области ИБ. Обзор международных и национальных стандартов и спецификаций в области ИБ: «Оранжевая книга», ИСО и др.

Цель работы: Изучить законодательный уровень информационной безопасности.

Теоретическое обоснование

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.

1.2.2. Закон "Об информации, информатизации и защите информации"

Основополагающим среди российских законов, посвященных вопросам информационной безопасности, следует считать закон "Об информации, информатизации и защите информации" от 20 февраля 1995 года номер 24-ФЗ (принят Государственной Думой 25 января 1995 года). В нем даются основные определения и намечаются направления развития законодательства в данной области.

Процитируем некоторые из этих определений:

- информация - сведения о лицах, предметах, фактах, событиях, явлениях и процессах независимо от формы их представления;
- документированная информация (документ) - зафиксированная на материальном носителе информация с реквизитами, позволяющими ее идентифицировать;
- информационные процессы - процессы сбора, обработки, накопления, хранения, поиска и распространения информации;
- информационная система - организационно упорядоченная совокупность документов (массивов документов) и информационных технологий, в том числе с использованием средств вычислительной техники и связи, реализующих информационные процессы;
- информационные ресурсы - отдельные документы и отдельные массивы документов, документы и массивы документов в информационных системах (библиотеках, архивах, фондах, банках данных, других информационных системах);
- информация о гражданах (персональные данные) - сведения о фактах, событиях и обстоятельствах жизни гражданина, позволяющие идентифицировать его личность;
- конфиденциальная информация - документированная информация, доступ к которой ограничивается в соответствии с законодательством Российской Федерации;

- пользователь (потребитель) информации - субъект, обращающийся к информационной системе или посреднику за получением необходимой ему информации и пользующийся ею.

Мы, разумеется, не будем обсуждать качество данных в Законе определений. Обратим лишь внимание на гибкость определения конфиденциальной информации, которая не сводится к сведениям, составляющим государственную тайну, а также на понятие персональных данных, закладывающее основу защиты последних.

Закон выделяет следующие цели защиты информации:

- предотвращение утечки, хищения, утраты, искажения, подделки информации;
- предотвращение угроз безопасности личности, общества, государства;
- предотвращение несанкционированных действий по уничтожению, модификации, искажению, копированию, блокированию информации;
- предотвращение других форм незаконного вмешательства в информационные ресурсы и информационные системы, обеспечение правового режима документированной информации как объекта собственности;
- защита конституционных прав граждан на сохранение личной тайны и конфиденциальности персональных данных, имеющихся в информационных системах;
- сохранение государственной тайны, конфиденциальности документированной информации в соответствии с законодательством;
- обеспечение прав субъектов в информационных процессах и при разработке, производстве и применении информационных систем, технологий и средств их обеспечения.

Отметим, что Закон на первое место ставит сохранение конфиденциальности информации. Целостность представлена также достаточно полно, хотя и на втором месте. О доступности ("предотвращение несанкционированных действий по ... блокированию информации") сказано довольно мало.

Продолжим цитирование:

"Защите подлежит любая документированная информация, неправомерное обращение с которой может нанести ущерб ее собственнику, владельцу, пользователю и иному лицу".

По сути, это положение констатирует, что защита информации направлена на обеспечение интересов субъектов информационных отношений.

Далее. "Режим защиты информации устанавливается:

- в отношении сведений, отнесенных к государственной тайне, - уполномоченными органами на основании Закона Российской Федерации "О государственной тайне";
- в отношении конфиденциальной документированной информации - собственником информационных ресурсов или уполномоченным лицом на основании настоящего Федерального закона;
- в отношении персональных данных - федеральным законом."

Здесь явно выделены три вида защищаемой информации, ко второму из которых принадлежит, в частности, коммерческая информация. Поскольку защите

подлежит только документированная информация, необходимым условием является фиксация коммерческой информации на материальном носителе и снабжение ее реквизитами. Отметим, что в данном месте Закона речь идет только о конфиденциальности; остальные аспекты ИБ забыты.

Обратим внимание, что защиту государственной тайны и персональных данных берет на себя государство; за другую конфиденциальную информацию отвечают ее собственники.

Как же защищать информацию? В качестве основного закон предлагает для этой цели мощные универсальные средства: лицензирование и сертификацию. Процитируем статью 19.

Информационные системы, базы и банки данных, предназначенные для информационного обслуживания граждан и организаций, подлежат сертификации в порядке, установленном Законом Российской Федерации "О сертификации продукции и услуг".

Информационные системы органов государственной власти Российской Федерации и органов государственной власти субъектов Российской Федерации, других государственных органов, организаций, которые обрабатывают документированную информацию с ограниченным доступом, а также средства защиты этих систем подлежат обязательной сертификации. Порядок сертификации определяется законодательством Российской Федерации.

Организации, выполняющие работы в области проектирования, производства средств защиты информации и обработки персональных данных, получают лицензии на этот вид деятельности. Порядок лицензирования определяется законодательством Российской Федерации.

Интересы потребителя информации при использовании импортной продукции в информационных системах защищаются таможенными органами Российской Федерации на основе международной системы сертификации.

Здесь трудно удержаться от риторического вопроса: а есть ли в России информационные системы без импортной продукции? Получается, что на защите интересов потребителей стоит в данном случае только таможня...

И еще несколько пунктов, теперь из статьи 22:

Владелец документов, массива документов, информационных систем обеспечивает уровень защиты информации в соответствии с законодательством Российской Федерации.

Риск, связанный с использованием несертифицированных информационных систем и средств их обеспечения, лежит на собственнике (владельце) этих систем и средств. Риск, связанный с использованием информации, полученной из несертифицированной системы, лежит на потребителе информации.

Собственник документов, массива документов, информационных систем может обращаться в организации, осуществляющие сертификацию средств защиты информационных систем и информационных ресурсов, для проведения анализа достаточности мер защиты его ресурсов и систем и получения консультаций.

Владелец документов, массива документов, информационных систем обязан оповещать собственника информационных ресурсов и (или) информационных систем о всех фактах нарушения режима защиты информации.

Из пункта 5 следует, что должны обнаруживаться все (успешные) атаки на ИС. Вспомним в этой связи один из результатов опроса (см. лекцию 1): около трети респондентов-американцев не знали, были ли взломаны их ИС за последние 12 месяцев. По нашему законодательству их можно было бы привлечь к ответственности...

Далее, статья 23 "Защита прав субъектов в сфере информационных процессов и информатизации" содержит следующий пункт:

Защита прав субъектов в указанной сфере осуществляется судом, арбитражным судом, третейским судом с учетом специфики правонарушений и нанесенного ущерба. Очень важными являются пункты статьи 5, касающиеся юридической силы электронного документа и электронной цифровой подписи:

Юридическая сила документа, хранимого, обрабатываемого и передаваемого с помощью автоматизированных информационных и телекоммуникационных систем, может подтверждаться электронной цифровой подписью.

Юридическая сила электронной цифровой подписи признается при наличии в автоматизированной информационной системе программно-технических средств, обеспечивающих идентификацию подписи, и соблюдении установленного режима их использования.

Право удостоверять идентичность электронной цифровой подписи осуществляется на основании лицензии. Порядок выдачи лицензий определяется законодательством Российской Федерации.

Таким образом, Закон предлагает действенное средство контроля целостности и решения проблемы "неотказуемости" (невозможности отказаться от собственной подписи).

Таковы важнейшие, на наш взгляд, положения Закона "Об информации, информатизации и защите информации". На следующей странице будут рассмотрены другие законы РФ в области информационной безопасности.

1.2.3. Другие законы и нормативные акты

Следуя логике Закона "Об информации, информатизации и защите информации", мы продолжим наш обзор Законом "О лицензировании отдельных видов деятельности" от 8 августа 2001 года номер 128-ФЗ (Принят Государственной Думой 13 июля 2001 года). Начнем с основных определений.

- "**Лицензия** - специальное разрешение на осуществление конкретного вида деятельности при обязательном соблюдении лицензионных требований и условий, выданное лицензирующим органом юридическому лицу или индивидуальному предпринимателю.
-
- **Лицензируемый вид деятельности** - вид деятельности, на осуществление которого на территории Российской Федерации требуется получение лицензии в соответствии с настоящим Федеральным законом.
-
- **Лицензирование** - мероприятия, связанные с предоставлением лицензий, переоформлением документов, подтверждающих наличие лицензий, приостановлением и возобновлением действия лицензий, аннулированием лицензий и контролем лицензирующих органов за соблюдением лицензиатами

при осуществлении лицензируемых видов деятельности соответствующих лицензионных требований и условий.

- **Лицензирующие органы** - федеральные органы исполнительной власти, органы исполнительной власти субъектов Российской Федерации, осуществляющие лицензирование в соответствии с настоящим Федеральным законом.

- **Лицензиат** - юридическое лицо или индивидуальный предприниматель, имеющие лицензию на осуществление конкретного вида деятельности."

Статья 17 Закона устанавливает перечень видов деятельности, на осуществление которых требуются лицензии. Нас будут интересовать следующие виды:

- распространение шифровальных (криптографических) средств;
- техническое обслуживание шифровальных (криптографических) средств;
- предоставление услуг в области шифрования информации;
- разработка и производство шифровальных (криптографических) средств, защищенных с использованием шифровальных (криптографических) средств информационных систем, телекоммуникационных систем;
- выдача сертификатов ключей электронных цифровых подписей, регистрация владельцев электронных цифровых подписей, оказание услуг, связанных с использованием электронных цифровых подписей и подтверждением подлинности электронных цифровых подписей;
- выявление электронных устройств, предназначенных для негласного получения информации, в помещениях и технических средствах (за исключением случая, если указанная деятельность осуществляется для обеспечения собственных нужд юридического лица или индивидуального предпринимателя);
- разработка и (или) производство средств защиты конфиденциальной информации;
- техническая защита конфиденциальной информации;
- разработка, производство, реализация и приобретение в целях продажи специальных технических средств, предназначенных для негласного получения информации, индивидуальными предпринимателями и юридическими лицами, осуществляющими предпринимательскую деятельность.

Необходимо учитывать, что, согласно статье 1, действие данного Закона не распространяется на следующие виды деятельности:

- деятельность, связанная с защитой государственной тайны;
- деятельность в области связи;
- образовательная деятельность.

Подчеркнем в этой связи, что данный Закон не препятствует организации Интернет-Университетом учебных курсов по информационной безопасности (не требует получения специальной лицензии; ранее подобная лицензия была необходима). В свою очередь, Федеральный Закон "Об образовании" не содержит каких-либо специальных положений, касающихся образовательной деятельности в области ИБ.

Основными лицензирующими органами в области защиты информации являются Федеральное агентство правительственной связи и информации (ФАПСИ) и Гостехкомиссия России. ФАПСИ ведает всем, что связано с криптографией, Гостехкомиссия лицензирует деятельность по защите конфиденциальной информации. Эти же организации возглавляют работы по сертификации средств соответствующей направленности. Кроме того, ввоз и вывоз средств криптографической защиты информации (шифровальной техники) и нормативно-технической документации к ней может осуществляться исключительно на основании лицензии Министерства внешних экономических связей Российской Федерации, выдаваемой на основании решения ФАПСИ. Все эти вопросы регламентированы соответствующими указами Президента и постановлениями Правительства РФ, которые мы здесь перечислять не будем.

В эпоху глобальных коммуникаций важную роль играет Закон "Об участии в международном информационном обмене" от 4 июля 1996 года номер 85-ФЗ (принят Государственной Думой 5 июня 1996 года). В нем, как и в Законе "Об информации...", основным защитным средством являются лицензии и сертификаты. Процитируем несколько пунктов из статьи 9.

Защита конфиденциальной информации государством распространяется только на ту деятельность по международному информационному обмену, которую осуществляют физические и юридические лица, обладающие лицензией на работу с конфиденциальной информацией и использующие сертифицированные средства международного информационного обмена.

Выдача сертификатов и лицензий возлагается на Комитет при Президенте Российской Федерации по политике информатизации, Государственную техническую комиссию при Президенте Российской Федерации, Федеральное агентство правительственной связи и информации при Президенте Российской Федерации. Порядок выдачи сертификатов и лицензий устанавливается Правительством Российской Федерации.

При обнаружении нештатных режимов функционирования средств международного информационного обмена, то есть возникновения ошибочных команд, а также команд, вызванных несанкционированными действиями обслуживающего персонала или иных лиц, либо ложной информацией собственник или владелец этих средств должен своевременно сообщить об этом в органы контроля за осуществлением международного информационного обмена и собственнику или владельцу взаимодействующих средств международного информационного обмена, в противном случае он несет ответственность за причиненный ущерб.

При желании здесь можно усмотреть обязательность выявления нарушителя информационной безопасности - положение, вне всяких сомнений, очень важное и прогрессивное.

Еще одна цитата - теперь из статьи 17 того же Закона.

Статья 17: "Сертификация информационных продуктов, информационных услуг, средств международного информационного обмена.

При ввозе информационных продуктов, информационных услуг в Российскую Федерацию импортер представляет сертификат, гарантирующий соответствие

данных продуктов и услуг требованиям договора. В случае невозможности сертификации ввозимых на территорию Российской Федерации информационных продуктов, информационных услуг ответственность за использование данных продуктов и услуг лежит на импортере.
Средства международного информационного обмена, которые обрабатывают документированную информацию с ограниченным доступом, а также средства защиты этих средств подлежат обязательной сертификации.
Сертификация сетей связи производится в порядке, определяемом Федеральным законом "О связи"."
Читая пункт 2, трудно удержаться от вопроса: "А нужно ли сертифицировать средства защиты средств защиты этих средств?" Ответ, конечно, положительный...
10 января 2002 года Президентом был подписан очень важный закон "Об электронной цифровой подписи" номер 1-ФЗ (принят Государственной Думой 13 декабря 2001 года), развивающий и конкретизирующий приведенные выше положения закона "Об информации...". Его роль поясняется в статье 1.
Целью настоящего Федерального закона является обеспечение правовых условий использования электронной цифровой подписи в электронных документах, при соблюдении которых электронная цифровая подпись в электронном документе признается равнозначной собственноручной подписи в документе на бумажном носителе.
Действие настоящего Федерального закона распространяется на отношения, возникающие при совершении гражданско-правовых сделок и в других предусмотренных законодательством Российской Федерации случаях. Действие настоящего Федерального закона не распространяется на отношения, возникающие при использовании иных аналогов собственноручной подписи.
Закон вводит следующие основные понятия:

- **Электронный документ** - документ, в котором информация представлена в электронно-цифровой форме.
- **Электронная цифровая подпись** - реквизит электронного документа, предназначенный для защиты данного электронного документа от подделки, полученный в результате криптографического преобразования информации с использованием закрытого ключа электронной цифровой подписи и позволяющий идентифицировать владельца сертификата ключа подписи, а также установить отсутствие искажения информации в электронном документе.
- **Владелец сертификата ключа подписи** - физическое лицо, на имя которого удостоверяющим центром выдан сертификат ключа подписи и которое владеет соответствующим закрытым ключом электронной цифровой подписи, позволяющим с помощью средств электронной цифровой подписи создавать свою электронную цифровую подпись в электронных документах (подписывать электронные документы).
- **Средства электронной цифровой подписи** - аппаратные и (или) программные средства, обеспечивающие реализацию хотя бы одной из следующих функций: создание электронной цифровой подписи в электронном документе с использованием закрытого ключа электронной цифровой подписи,

подтверждение с использованием открытого ключа электронной цифровой подписи подлинности электронной цифровой подписи в электронном документе, создание закрытых и открытых ключей электронных цифровых подписей.

- **Сертификат средств электронной цифровой подписи** - документ на бумажном носителе, выданный в соответствии с правилами системы сертификации для подтверждения соответствия средств электронной цифровой подписи установленным требованиям.
- **Закрытый ключ электронной цифровой подписи** - уникальная последовательность символов, известная владельцу сертификата ключа подписи и предназначенная для создания в электронных документах электронной цифровой подписи с использованием средств электронной цифровой подписи.
- **Открытый ключ электронной цифровой подписи** - уникальная последовательность символов, соответствующая закрытому ключу электронной цифровой подписи, доступная любому пользователю информационной системы и предназначенная для подтверждения с использованием средств электронной цифровой подписи подлинности электронной цифровой подписи в электронном документе.
- **Сертификат ключа подписи** - документ на бумажном носителе или электронный документ с электронной цифровой подписью уполномоченного лица удостоверяющего центра, которые включают в себя открытый ключ электронной цифровой подписи и выдаются удостоверяющим центром участнику информационной системы для подтверждения подлинности электронной цифровой подписи и идентификации владельца сертификата ключа подписи.

Подтверждение подлинности электронной цифровой подписи в электронном документе - положительный результат проверки соответствующим сертифицированным средством электронной цифровой подписи с использованием сертификата ключа подписи принадлежности электронной цифровой подписи в электронном документе владельцу сертификата ключа подписи и отсутствия искажений в подписанном данной электронной цифровой подписью электронном документе.

Пользователь сертификата ключа подписи - физическое лицо, использующее полученные в удостоверяющем центре сведения о сертификате ключа подписи для проверки принадлежности электронной цифровой подписи владельцу сертификата ключа подписи.

Информационная система общего пользования - информационная система, которая открыта для использования всеми физическими и юридическими лицами и в услугах которой этим лицам не может быть отказано.

Корпоративная информационная система - информационная система, участниками которой может быть ограниченный круг лиц, определенный ее владельцем или соглашением участников этой информационной системы.

Пересказать такие определения своими словами невозможно... Обратим внимание на неоднозначное использование термина "сертификат", которое, впрочем, не должно привести к путанице. Кроме того, данное здесь определение электронного документа слабее, чем в Законе "Об информации...", поскольку нет упоминания реквизитов.

Согласно Закону, электронная цифровая подпись в электронном документе равнозначна собственноручной подписи в документе на бумажном носителе при одновременном соблюдении следующих условий:

- сертификат ключа подписи, относящийся к этой электронной цифровой подписи, не утратил силу (действует) на момент проверки или на момент подписания электронного документа при наличии доказательств, определяющих момент подписания;
- подтверждена подлинность электронной цифровой подписи в электронном документе;
- электронная цифровая подпись используется в соответствии со сведениями, указанными в сертификате ключа подписи.

Закон определяет сведения, которые должен содержать сертификат ключа подписи:

- уникальный регистрационный номер сертификата ключа подписи, даты начала и окончания срока действия сертификата ключа подписи, находящегося в реестре удостоверяющего центра;
- фамилия, имя и отчество владельца сертификата ключа подписи или псевдоним владельца. В случае использования псевдонима запись об этом вносится удостоверяющим центром в сертификат ключа подписи;
- открытый ключ электронной цифровой подписи;
- наименование средств электронной цифровой подписи, с которыми используется данный открытый ключ электронной цифровой подписи;
- наименование и местонахождение удостоверяющего центра, выдавшего сертификат ключа подписи;
- сведения об отношениях, при осуществлении которых элетронный документ с электронной цифровой подписью будет иметь юридическое значение.

Интересно, много ли Федеральных законов, содержащих такое количество технической информации и столь зависимых от конкретной технологии?

На этом мы заканчиваем обзор законов РФ, относящихся к информационной безопасности.

1.3. Обзор зарубежного законодательства в области информационной безопасности

Конечно, излишняя амбициозность заголовка очевидна. Разумеется, мы лишь пунктиром очертим некоторые законы нескольких стран (в первую очередь - США), поскольку только в США таких законодательных актов около 500.

Ключевую роль играет американский "Закон об информационной безопасности" (Computer Security Act of 1987, Public Law 100-235 (H.R. 145), January 8, 1988). Его цель - реализация минимально достаточных действий по обеспечению безопасности информации в федеральных компьютерных системах, без ограничений всего спектра возможных действий.

Характерно, что уже в начале Закона называется конкретный исполнитель - Национальный институт стандартов и технологий (НИСТ), отвечающий за выпуск стандартов и руководств, направленных на защиту от уничтожения и несанкционированного доступа к информации, а также от краж и подлогов, выполняемых с помощью компьютеров. Таким образом, имеется в виду как

регламентация действий специалистов, так и повышение информированности всего общества.

Согласно Закону, все операторы федеральных ИС, содержащих конфиденциальную информацию, должны сформировать **планы обеспечения ИБ.** Обязательным является и периодическое обучение всего персонала таких ИС.

НИСТ, в свою очередь, обязан проводить исследования природы и масштаба уязвимых мест, вырабатывать экономически оправданные меры защиты. Результаты исследований рассчитаны на применение не только в государственных системах, но и в частном секторе.

Закон обязывает НИСТ координировать свою деятельность с другими министерствами и ведомствами, включая Министерство обороны, Министерство энергетики, Агентство национальной безопасности (АНБ) и т.д., чтобы избежать дублирования и несовместимости.

Помимо регламентации дополнительных функций НИСТ, Закон предписывает создать при Министерстве торговли комиссию по информационной безопасности, которая должна:

- выявлять перспективные управленческие, технические, административные и физические меры, способствующие повышению ИБ;
- выдавать рекомендации Национальному институту стандартов и технологий, доводить их до сведения всех заинтересованных ведомств.

С практической точки зрения важен раздел 6 Закона, обязывающий все правительственные ведомства сформировать план обеспечения информационной безопасности, направленный на то, чтобы компенсировать риски и предотвратить возможный ущерб от утери, неправильного использования, несанкционированного доступа или модификации информации в федеральных системах. Копии плана направляются в НИСТ и АНБ.

В 1997 году появилось продолжение описанного закона - законопроект "О совершенствовании информационной безопасности" (Computer Security Enhancement Act of 1997, H.R. 1903), направленный на усиление роли Национального института стандартов и технологий и упрощение операций с криптосредствами.

В законопроекте констатируется, что частный сектор готов предоставить криптосредства для обеспечения конфиденциальности и целостности (в том числе аутентичности) данных, что разработка и использование шифровальных технологий должны происходить на основании требований рынка, а не распоряжений правительства. Кроме того, здесь отмечается, что за пределами США имеются сопоставимые и общедоступные криптографические технологии, и это следует учитывать при выработке экспортных ограничений, чтобы не снижать конкурентоспособность американских производителей аппаратного и программного обеспечения.

Для защиты федеральных ИС рекомендуется более широко применять технологические решения, основанные на разработках частного сектора. Кроме того, предлагается оценить возможности общедоступных зарубежных разработок.

Очень важен раздел 3, в котором от НИСТ требуется по запросам частного сектора готовить добровольные стандарты, руководства, средства и методы для

инфраструктуры открытых ключей (см. выше Закон РФ об ЭЦП), позволяющие сформировать негосударственную инфраструктуру, пригодную для взаимодействия с федеральными ИС.

В разделе 4 особое внимание обращается на необходимость анализа средств и методов оценки уязвимых мест других продуктов частного сектора в области ИБ. Приветствуется разработка правил безопасности, нейтральных по отношению к конкретным техническим решениям, использование в федеральных ИС коммерческих продуктов, участие в реализации шифровальных технологий, позволяющее в конечном итоге сформировать инфраструктуру, которую можно рассматривать как резервную для федеральных ИС.

Важно, что в соответствии с разделами 10 и далее предусматривается выделение конкретных (и немалых) сумм, называются точные сроки реализации программ партнерства и проведения исследований инфраструктуры с открытыми ключами, национальной инфраструктуры цифровых подписей. В частности, предусматривается, что для удостоверяющих центров должны быть разработаны типовые правила и процедуры, порядок лицензирования, стандарты аудита.

В 2001 году был одобрен Палатой представителей и передан в Сенат новый вариант рассмотренного законопроекта - Computer Security Enhancement Act of 2001 (H.R. 1259 RFS). В этом варианте примечательно как то, что, по сравнению с предыдущей редакцией, было убрано, так и то, что добавилось.

За четыре года (1997-2001 гг.) на законодательном и других уровнях информационной безопасности США было сделано многое. Смягчены экспортные ограничения на криптосредства (в январе 2000 г.). Сформирована инфраструктура с открытыми ключами. Разработано большое число стандартов (например, новый стандарт электронной цифровой подписи - FIPS 186-2, январь 2000 г.). Все это позволило не заострять более внимания на криптографии как таковой, а сосредоточиться на одном из ее важнейших приложений - аутентификации, рассматривая ее по отработанной на криптосредствах методике. Очевидно, что, независимо от судьбы законопроекта, в США будет сформирована национальная инфраструктура электронной аутентификации. В данном случае законотворческая деятельность идет в ногу с прогрессом информационных технологий.

Программа безопасности, предусматривающая экономически оправданные защитные меры и синхронизированная с жизненным циклом ИС, упоминается в законодательстве США неоднократно. Согласно пункту 3534 ("Обязанности федеральных ведомств") подглавы II ("Информационная безопасность") главы 35 ("Координация федеральной информационной политики") рубрики 44 ("Общественные издания и документы"), такая программа должна включать:

- периодическую оценку рисков с рассмотрением внутренних и внешних угроз целостности, конфиденциальности и доступности систем, а также данных, ассоциированных с критически важными операциями и ресурсами;
- правила и процедуры, позволяющие, опираясь на проведенный анализ рисков, экономически оправданным образом уменьшить риски до приемлемого уровня;

- обучение персонала с целью информирования о существующих рисках и об обязанностях, выполнение которых необходимо для их (рисков) нейтрализации;
- периодическую проверку и (пере)оценку эффективности правил и процедур;
- действия при внесении существенных изменений в систему;
- процедуры выявления нарушений информационной безопасности и реагирования на них; эти процедуры должны помочь уменьшить риски, избежать крупных потерь; организовать взаимодействие с правоохранительными органами.

Конечно, в законодательстве США имеются в достаточном количестве и положения ограничительной направленности, и директивы, защищающие интересы таких ведомств, как Министерство обороны, АНБ, ФБР, ЦРУ, но мы не будем на них останавливаться. Желающие могут прочитать раздел "Законодательная база в области защиты информации" в превосходной статье О. Беззубцева и А. Ковалева "О лицензировании и сертификации в области защиты информации" (Jet Info, 1997, 4).

В законодательстве ФРГ выделим весьма развернутый (44 раздела) Закон о защите данных (Federal Data Protection Act of December 20, 1990 (BGBl.I 1990 S.2954), amended by law of September 14, 1994 (BGBl. I S. 2325)). Он целиком посвящен защите персональных данных.

2. Порядок выполнения работы

1.Ознакомиться с российским зарубежным законодательством в области ИБ..
2.Выполнить практическое задание.
3.Ответить на контрольные вопросы.

Практическое занятие №3

«Системы менеджмента качества»

Цель: Изучить ГОСТ ИСО 9000-2011 «Системы менеджмента качества. Требования»; определить основные термины и понятия системы менеджмента качества.

Задание. Составить глоссарий ГОСТ ИСО 9000-2011 «Системы менеджмента качества. Требования».

Ход работы

1. Глоссарий - (лат. glossarium — «собрание глосс») — словарь узкоспециализированных терминов в какой-либо отрасли знаний с толкованием, иногда переводом на другой язык, комментариями и примерами.
2. Изучить ГОСТ ИСО 9000-2011 «Системы менеджмента качества. Требования» (Приложение 2).
3. Составить глоссарий в виде таблицы.

Таблица.

№ п/п	Термин	Определение	Примечание
1			
2			
3…			

4. Ответить на контрольные вопросы.

Контрольные вопросы

1. Сфера применения ГОСТ ИСО 9000-2011 «Системы менеджмента качества. Требования»?
2. Определите вид стандарта ГОСТ ИСО 9000-2011 «Системы менеджмента качества. Требования».
3. Сформулируйте принципы менеджмента качества.
4. В чем состоит сущность управления качеством продукции?
5. Поясните генезис и проблематику менеджмента качества.

Общие выводы по занятию:

_____
_____
_____

Практическое занятие № 4

Цель работы: изучить схемы сертификации продукции.

Порядок выполнения работы:

1. Изучить теоретическую часть методических указаний;
2. Ответить на контрольные вопросы письменно;
3. Сделать выводы по проделанной работе.

Теоретическое обоснование

Схемы сертификации — это определенный порядок действий, соответствии с которым проводится процедура сертификации качества продукции.

Схема сертификации 1 - проводится испытание в аккредитованной испытательной лаборатории изделия, то есть, типового образца. Данная схема применяется для изделий сложной конструкции.

Схема сертификации 1 предназначена для ограниченного объема выпуска отечественной продукции и поставляемой по контракту импортируемой продукции. Схема сертификации 1а включает дополнение к схеме 1 — это анализ состояния производства.

Схема сертификации 2 - проводится испытание образцов продукции, после чего заявитель уже может оформить сертификат соответствия. В данной схеме сертификации предусмотрен инспекционный контроль. Для этого образец продукции отбирается в торговых организациях, реализующих данный товар, и подвергается испытаниям в аккредитованной испытательной лаборатории.

Схема сертификации 2а включает дополнение к схеме 2 — анализ состояния производства до выдачи сертификата.
Схемы сертификации продукции 2 и 2а рекомендуются для импортируемой продукции, поставляемой на постоянной основе.
Схема сертификации 3 предусматривает испытания образца, но без анализа производства, а после выдачи сертификата - инспекционный контроль путем испытания образца продукции перед отправкой потребителю. Образец испытывается в аккредитованной испытательной лаборатории.
Схема сертификации 3а предусматривает обязательное испытание образца продукции и анализ состояния производства, а также инспекционный контроль в такой же форме.
Схемы сертификации продукции 3 и 3а подходят для продукции, стабильность качества которой соблюдается в течение длительного периода времени.
Схема сертификации 4 заключается в испытании типового образца, как в предыдущих схемах, с несколько иным инспекционным контролем: образцы для испытаний отбираются как со склада изготовителя, так и у продавца. Модифицированная схема 4а в дополнение к схеме 4 включает анализ состояния производства до выдачи сертификата соответствия на продукцию. Данную схему сертификации используют в случаях, когда нецелесообразно не проводить инспекционный контроль.
Схема сертификации 5 — это испытания образца продукции, анализ производства путем подтверждения соответствия системы обеспечения качества или самого производства, а также проведение инспекционного контроля: испытание образцов продукции, отобранных у продавца и у изготовителя, и в дополнение проверка стабильности условий производства и действующей системы управления качеством.
Схема сертификации 6 заключается в контроле на предприятии системы качества, но если сертификат системы качества предприятие уже имеет, ему достаточно представить заявление-декларацию. Это обычно установлено в правилах системы сертификации однородной продукции.
Схема сертификации 7 подразумевает обязательное проведение испытаний. Это значит, что в партии продукции, отбирается образец по установленным правилам, который проходит испытания в аккредитованной лаборатории с последующей процедурой выдачи сертификата соответствия. Инспекционный контроль не предусмотрен.
Схема сертификации 8 - проведение испытания каждого образца продукции, изготовленного предприятием, в аккредитованной испытательной лаборатории и выдача сертификата соответствия в случае положительных результатов испытаний.
Схемы сертификации 9-10а, которые опираются на заявление изготовителя с последующим инспекционным контролем продукции.
Схема сертификации 9 предназначена для продукции, выпускаемой непостоянно. Это может быть продукция отечественного производства.

Схемы сертификации 10 и 10а применяются для оценки качества продукции, производимой ограниченными партиями, но в течение продолжительного периода времени.

2. ПРАКТИЧЕСКАЯ ЧАСТЬ

1. Ответить на контрольные вопросы письменно:

1. Что такое схемы сертификации?
2. Для каких изделий применяется схема сертификации 1?
3. Для какой продукции рекомендуются схемы сертификации 2 и 2а?
4. Для какой продукции подходят схемы сертификации 3 и 3а?
5. В чем заключается схема сертификации 6?
6. Для какой продукции предназначена схема сертификации 9?

2. Сделать выводы по проделанной работе.

Практическое занятие № 5

Выборка и составление схемы сертификации для специальности информационные систем

Цель: Изучить правила проведения сертификации информационно-программных средств.

Задание:

1. Изучить и описать порядок проведения сертификации информационно-программных средств.
2. Изучить и заполнить документы, необходимые для проведения сертификации информационно-программных средств. (Комплект документов для проведения сертификации программных средств располагается в папке Документы для сертификации, которая находится в папке Мои документы).

Ход занятия:

1. Изучить теоретический материал по заданной теме.
2. Заполнить шаблоны документов на проведение сертификации информационно-программных средств.
3. Оформить отчет по практическому занятию. В отчет включить заполненные документы и ответы на контрольные вопросы.

Теоретическое обоснование

Порядок проведения сертификации программного обеспечения

Процедуры и вся технология проведения работ по сертификации определяются схемой сертификации, которая устанавливает четкую совокупность действий, по результатам которых принимается решение о соответствии или несоответствии продукции заданным требованиям. Согласно идеологии Международной организации по стандартизации (ИСО) общепризнанными являются восемь основных схем сертификации. Они используются и в комплекте основополагающих документов системы сертификации ГОСТ Р. При этом число схем сертификации, принятых Госстандартом России, в два раза больше, чем

принято в зарубежной и международной практике. Схемы сертификации, принятые в системе сертификации ГОСТ Р, приведены в приложении 1.

Для каждой схемы сертификации продукции приводятся условия ее применения с учетом степени опасности продукции. При проведении сертификации программного обеспечения наиболее удобно применение схемы 10а. Госстандартом России предусматривается ее использование в качестве доказательства соответствия (несоответствия) продукции (программного обеспечения) установленным требованиям декларации, о соответствии прилагаемым к ней документам, подтверждающим соответствие продукции установленным требованиям.

Порядок проведения сертификации программного обеспечения средств измерений, информационно-измерительных систем и аппаратно-программных комплексов определен такими методиками как МИ 2891-2004 "ГСИ. Общие требования к программному обеспечению средств измерений" и МИ 2955-2005 "Типовая методика аттестации программного обеспечения средств измерений и порядок ее проведения".

Кроме того, в настоящее время в связи с принятием 11 июня 2008 г. новой редакции Закона РФ "Об обеспечении единства измерений", где в статье 9, п. 1 говорится о том, что "в состав обязательных требований к средствам измерений …в необходимых случаях включаются также требования к … программному обеспечению", ФГУП ВНИИМС приступил к разработке национального стандарта ГОСТ Р "ГСИ. Требования к программному обеспечению средств измерений и информационно - измерительных систем".

Порядок проведения сертификации программного обеспечения включает:

- подачу заявки на сертификацию;
- принятие решения по заявке на сертификацию, в том числе назначение экспертов на проведение основных работ по сертификации из числа экспертов органа по сертификации;
- оформление договора на проведение работ по сертификации;
- проведение сертификационной проверки ПО, в том числе при необходимости проведение испытаний/контроля ПО по согласованным с заказчиком методикам;
- принятие решения о выдаче Сертификата соответствия и разрешения использования знака соответствия либо об отказе в выдаче Сертификата соответствия;
- выдача Сертификата соответствия и разрешения использования знака соответствия;
- занесение заявителя/изготовителя ПО и перечня сертифицированных ПО в Реестр СДС ПО;
- проведение инспекционного контроля сертифицированных ПО.

Результатом сертификации является возможность приобрести программный продукт в Российской Федерации с соответствующей поддержкой от производителя или его официального представителя.

В результате проведенной сертификации производитель ПО получает:

– Экспертное заключение;
– Свидетельство о сертификации;
– Право использовать логотип «Проверено IT Expert».

Сертификация выгодна и для покупателей соответствующего программного обеспечения. Покупатель получит:

– Предметную оценку функционала программного обеспечения;
– Возможность сравнения продуктов между собой;
– Возможность самостоятельной оценки продуктов по своим критериям.

Перечень информации предоставляемой заявителем для прохождения процедуры сертификации

-описание структуры сертифицируемого программного обеспечения, выполняемых функций, в том числе последовательность обработки данных;
-описание функций сертифицируемого ПО и параметров программного обеспечения, существенных для их работы;
-описание реализованных в сертифицируемом программном обеспечении алгоритмов функционирования, в том числе вычислительных алгоритмов, а также их блок-схемы;
-описание модулей программного обеспечения;
-перечень интерфейсов и перечень команд для каждого интерфейса, включая заявление об их полноте;
-список, значение и действие всех команд, получаемых от устройств ввода (клавиатуры, мыши, сенсорных устройств и т.п.);
-описание реализованных методов идентификации сертифицируемого программного обеспечения;
-описание реализованных методов защиты сертифицируемого программного обеспечения и данных от влияющих факторов;
-описание интерфейсов пользователя, всех меню и диалогов;
-описание хранимых или передаваемых наборов данных;
-руководство пользователя на сертифицируемое программное обеспечение;
-характеристики необходимых системных и аппаратных средств, если эта информация не приведена в руководстве пользователя.

Перечень документов, сопровождающих программное обеспечение, может корректироваться соглашением между исполнителем и заказчиком сертификации ПО.

Приложение 1. Бланк заявки на проведение сертификации
Приложение 2. Бланк договора на проведение сертификации

Контрольные вопросы

1. Что такое сертификация программной продукции?
2. Что означает термин "программная продукция" и почему говорится о сертификации программной продукции, а не программных средств или программ?

3. Является ли сертификация программной продукции обязательной?
4. Что относится к нормативным документам, на соответствие которым проводится сертификация?
5. Какие материалы нужно представить на сертификацию и кто это может сделать?
6. Что в заявке на сертификацию означает фраза "Схема сертификации №3"?
7. Что включает в себя процесс сертификации?
8. Как проводится проверка соответствия ПС разделам и пунктам нормативных документов?
9. Срок действия сертификата соответствия?
10. В каких случаях сертификат приостанавливается или отменяется?
11. Какие виды программных средств могут быть сертифицированы в ОС ПС?
12. Сколько продолжается процесс сертификации?
13. Чем сертификат отличается от лицензии?
14. Какая копия сертификата считается действительной?
15. Что означает «Сертифицируемый объем ПС», упомянутый в заявке?
16. Может ли быть сертифицировано зарубежное программное средство?

Практическое занятие № 6

«Основные виды технической и технологической документации»

Цель занятия: познакомить обучающихся с видами нормативной технической документации (ЕСТД и ЕСКД), их использованием в производстве для стандартизации технической и конструкторской документации.

Порядок проведения занятия: группа обучающихся раскрывает понятия нормативных документов и стандартов предприятий.

Теоретическое обоснование:

Стандарты предприятия - разрабатываются и принимаются самими предприятиями. Объектом стандартизации в этом случае обычно являются составляющие организации и управления производством, совершенствование которых - главная цель стандартизации на данном уровне.

Закон РФ «О стандартизации» рекомендует использовать стандартизацию на предприятии для освоения данным конкретным предприятием государственных, международных, региональных стандартов,
а также для регламентирования требований к сырью, полуфабрикатам, закупаемых у других организаций.

Задание 1. Раскрыть понятия.

Обучающиеся по заданию преподавателя, используя основную и дополнительную литературу рассматривают основные понятия: Стандартизация, нормативный документ, ГОСТ, ГОСТ Р, ОСТ, ТУ, СТП, Технический регламент. Указывают содержание и назначение каждого наименования стандартов, и примерный объем стандартов, используемых в технологии компьютерных сетей.

Стандартизация

Нормативный документ -

ГОСТ – Государственный межнациональный стандарт

ГОСТ Р- Государственный национальный стандарт

ОСТ – Отраслевой стандарт

ТУ – технические условия

СТП – стандарты предприятий

Взаимозаменяемость –

Технический регламент -

Общие выводы по занятию

_____

_____

_____

Практическое занятие №7

ЕСКД. ГОСТ 2.101-93. ГОСТ 2.104-68 ЕСКД Основные надписи. Оформление основной надписи, рамок, колонтитулов. Оформление спецификации сборочного чертежа согласно ГОСТ 2. 108-68

Цель работы: закрепить умения при оформлении регламентов и протоколов

Основные теоретические сведения

При принятии решения о реализации любого проекта по внедрению информационной системы (ИС) важной задачей является оценка эффективности инвестиций в такой проект. Кроме того, существует необходимость в реализации единой ИТ-стратегии предприятия, которая позволит адекватно сочетать развитие как программной, так и аппаратной части системы параллельно с комплексом работ по развитию существующей ИТ-инфраструктуры. В данном случае становится актуальной проблема жизненного цикла, как комплекса программных средств, так и самой ИС. Жизненный цикл программных средств (ПС) в стандартах представляет собой набор этапов, частных работ и операций в последовательности их выполнения и взаимосвязях, регламентирующих ведение работ от подготовки технического задания до завершения испытаний ряда версий и окончания эксплуатации ПС или ИС. Стандарты включают правила описания исходной информации, способов и методов выполнения операций, устанавливают контроль технологических процессов, требования к оформлению их результатов, а также регламентируют содержание технологических и эксплуатационных документов на комплексы программ. Они определяют организационную структуру коллектива, обеспечивают распределение и планирование заданий, а также контроль за этапами создания комплекса ПС. В России разработка и испытания автоматизированных систем (АС), в частности ПС, регламентированы ГОСТ 34.601-90. Стадии создания АС; ГОСТ 34.602-89. ТЗ на создание АС; ГОСТ 34.603-92. Виды испытаний АС. Однако создание, сопровождение и развитие прикладных ПС для современных ИС в этих стандартах отражены недостаточно, а отдельные их положения устарели, с точки зрения построения современных распределенных комплексов прикладных программ высокого качества в системах управления и обработки данных с различной архитектурой. Поэтому целесообразно выбирать и использовать апробированные зарубежные стандарты в этой области, а также адаптировать их под реализацию конкретного проекта. Основные современные зарубежные стандарты ориентированы на описание жизненного цикла сложных ПС обработки информации и управления в реальном времени. Однако используемые в настоящее время в компаниях жизненные циклы

ПС в последнее время зачастую отличаются от приведенных в стандартах в связи с развитием и внедрением объектно- ориентированного анализа и проектирования, а также методов быстрой разработки прикладных программ, CASE-систем и языков четвертого поколения. В новых технологиях сокращаются стадии непосредственного создания программных и 9 информационных компонентов и детализируются процессы системного анализа и проектирования ПС в целом. Целесообразно рассмотреть проблему определения требований к ИС предприятия: выбора модели жизненного цикла (ЖЦ) разработки, определения контрактных условий реализации проекта, выбор нотации и инструментального средства формализованного описания требований. Необходимость определения требований к ИС возникает в следующих случаях: в момент выбора новой ИС, при подготовке тендерной документации, заключении договора на разработку или дополнительную надстройку выбранной ИС, уточнении (детализации) потребностей бизнеса в процессе разработки или надстройки системы, а также необходимости внесения изменений в систему в ходе эксплуатации. В каждом случае перед специалистами предприятия и организации встает задача выбора уровня детализации требований, методов описания, включая формализованное описание с использованием графического моделирования. На уровень детализации, область определения, а также используемые методы описания влияют: выбранная модель ЖЦ разработки и внедрения; характер разрабатываемого и внедряемого ПО (заказная разработка, настройка ИС, согласно требованиям заказчика); используемые средства и методы проектирования (в случае заказной разработки). Модель жизненного цикла представляет собой структуру, содержащую процессы, действия и задачи, которые осуществляются в ходе разработки, функционирования и сопровождения программного продукта (ПП) в течение всей жизни системы, от определения требований до вывода из эксплуатации. Существует несколько моделей и стандартов, а также концепций и методологий, в той или иной степени регламентирующих жизненный цикл, большинство из них относятся к заказному ПО, АС и др. Кроме непосредственно жизненного цикла в данных стандартах и методиках регламентируют также и процессы разработки. Рассмотрим базовые стандарты и методологии, регламентирующие жизненный цикл ПС и ИС в целом. Стандарты комплекса ГОСТ 34. Эти стандарты на создание и развитие АС - обобщенные, но воспринимаемые как весьма жесткие по структуре ЖЦ и проектной документации. ГОСТ 34.601-90 распространяется на АС и устанавливает стадии и этапы их создания. Кроме того, в стандарте содержится описание работ на каждом этапе. Стадии и этапы, закрепленные в стандарте, в большей степени соответствуют каскадной модели жизненного цикла. Изначально ГОСТ 34 задумывался в конце 1980-х годов как всеобъемлющий комплекс взаимосвязанных межотраслевых документов. Объектами стандартизации являются АС различных видов и все виды их компонентов, а не только ПО и базы данных (БД). Комплекс рассчитан на взаимодействие заказчика и разработчика. Аналогично ISO 12207 предусмотрено, что заказчик может разрабатывать АС для себя самостоятельно (если создаст для этого специализированное подразделение). Поскольку ГОСТ 34 в основном уделяет

внимание содержанию проектных документов, распределение действий между сторонами обычно делается, исходя из этого содержания. 10 В стандарте описано содержание документов, разрабатываемых на каждом этапе. Это определяет потенциальные возможности выделения на содержательном уровне сквозных работ, выполняемых параллельно или последовательно, и составляющих их задач. Такой прием может использоваться при построении профиля стандартов ЖЦ проекта, включающего согласованные подмножества стандартов ГОСТ 34 и ISO 12207. Международный стандарт ISO/IEC 12207. Первая редакция ISO 12207 была подготовлена в 1995 году объединенным техническим комитетом ISO/IEC JTC1 "Информационные технологии, подкомитет SC7, проектирование программного обеспечения". По определению, ISO12207 — базовый стандарт процессов ЖЦ ПО, ориентированный на различные виды ПО и типы проектов АС, куда ПО входит как часть. Стандарт определяет стратегию и общий порядок в создании и эксплуатации ПО, он охватывает ЖЦ ПО от концептуализации идей до завершения ЖЦ. Очень важное замечание стандарта: процессы, используемые во время ЖЦ ПО, должны быть совместимы с процессами, используемыми во время ЖЦ АС. (Отсюда понятна целесообразность совместного использования стандартов на АС и ПО.) Определение стандарта: система - это объединение одного или более процессов, аппаратных средств, программного обеспечения, оборудования и людей для обеспечения возможности удовлетворения определенных потребностей или целей. Стандарт ISO 12207 равносильно ориентирован на организацию действий каждой из двух сторон: поставщик (разработчик) и покупатель (пользователь). Может быть в равной степени применен, когда обе стороны из одной организации. Процессы ЖЦ. Стандарт ISO состоит из крупных обобщенных процессов: "приобретение", "поставка", "разработка" и т.п. Каждый процесс разделен на набор действий, любое действие - на комплекс задач. Очень важное отличие ISO: любой процесс, действие или задача инициируется и выполняется другим процессом по мере необходимости, причем нет заранее определенных последовательностей (естественно, при сохранении логики связей по исходным сведениям задач и т.п.). Динамический характер стандарта зависит от способа определения последовательности выполнения процессов и задач, при котором один процесс при необходимости вызывает другой или его часть. Стандарт определяет архитектуру, процессы, разделы и подразделы ЖЦ ПС, а также перечень базовых работ и детализирует содержание каждой из них. Архитектура ЖЦ ПС в стандарте базируется на трех крупных компонентах (см. рисунок 1.1). Стандарт принципиально не содержит конкретные методы действий, тем более - заготовки решений или документации. Он описывает архитектуру процессов ЖЦ ПО, но не конкретизирует в деталях, как реализовать или выполнить услуги и задачи, включенные в процессы, не предназначен для предписания имени. Стандарт не предписывает конкретную модель ЖЦ или метод разработки ПО, но определяет, что стороны - участники использования стандарта ответственны за выбор модели ЖЦ для проекта ПО, за адаптацию процессов и задач стандарта к этой модели, за выбор и применение методов разработки ПО, за выполнение действий и задач, подходящих для проекта ПО.

Порядок выполнения работы

1. Систематизировать комплекс государственных и международных стандартов, регламентирующих процессы разработки ИС, заполнив таблицу - Стандарты по разработке информационных систем.

Обозначение стандарта	Наименование стандарта
Российские (стандарты СССР)	
Российские, идентичные международным	

1. Дать краткую характеристику основных международных методологий и стандартов, применяющихся при создании, эксплуатации и аудите ИС, заполнив таблицу.

Таблица - Международные методологии и стандарты

Наименование	Расшифровка (англ)	Назначение
IDEF		
ITSM и ITIL		
ИСО-ИЭК 15504		
ИСО-ИЭК 12207		
Cobit		

2. Изучить ГОСТ 34.201-89 "Виды, комплектность и обозначение документов при создании автоматизированных систем". Описать виды и назначение документов, разрабатываемых на стадиях "Эскизный проект", "Технический проект", "Рабочая документация", заполнив таблицу.

Таблица - Виды и назначение документов по ГОСТ 34.201-89

Вид документа	Код документа	Назначение документа

3. Изучить ГОСТ 34.601-90 "Автоматизированные системы стадии создания". Составить таблицу.

Таблица - Стадии и этапы создания АС

Стадии	Этапы работ
1.	1.1 1.2
2.	2.1 2.2

4. Классифицировать законодательные акты в области информационных систем и технологий в соответствии с критериями, обозначенными в таблице.

Таблица - Нормативно-правовое обеспечение информационной деятельности

Раздел	Перечень документов

Основные нормативно- правовые акты Информационного права	1 2
Основное законодательство о программах для ЭВМ (и БД)	1 2
Законодательство, связанное с Интернет-деятельностью	1 2
Подзаконные акты	1 2

6. В сети интернет найти Гражданский кодекс (ч. 4,), изучить Главу 69. "Общие положения" Раздела VII. "Права на результаты интеллектуальной деятельности и средства индивидуализации". Дать письменный ответ на вопрос: Какие объекты интеллектуальной собственности, касающиеся области ИТ, являются объектом правового регулирования гл. 69 Гражданского кодекса?
7. В сети интернет найти Федеральный закон от 27 июля 2006 г. № 149-ФЗ "Об информации, информационных технологиях и защите информации". Дать письменный ответ на вопрос: Какие виды ответственности за правонарушения в сфере информации, информационных технологий и защиты информации предусмотрены данным Федеральным законом?
8. Составить отчет.

Содержание отчета

1. Заголовок, содержащий № ПР, тему, цель работы.
2. Таблица 1.1.
3. Таблица 1.2.
4. Таблица 1.3. 5
. Таблица 1.4.
6. Таблица 1.5.
7. Ответ на вопрос п.6.
8. Ответ на вопрос п.7.
9. Выводы по работе.

Контрольные вопросы

1. Какие группы стандартов применяются в сфере создания и эксплуатации ИС?
2. Что означает ИСО(ISO)/МЭК(IEC) в маркировке стандарта?
3. Назовите стадии создания АС согласно ГОСТ 34.601-90
4. Что представляет собой техническое задание на создание автоматизированной системы в соответствии с ГОСТ 34.602-89?
5. Какие виды испытаний автоматизированных систем предусмотрены ГОСТ 34.603-92?
6. Сформулируйте модель жизненного цикла ИС по стандарту Cobit.
7. Каково назначение стандарта Cobit?
8. В чем особенность методологии ITSM?
9. Какие основные нормативные документы регулируют правоотношения в области ИТ?

4. ИНФОРМАЦИОННОЕ ОБЕСПЕЧЕНИЕ ПРАКТИЧЕСКИХ РАБОТ

Основная литература:

Основные:

1. Пухоренко Ю. В., Метрология, стандартизация, сертификация: учебное пособие/ Пухоренко Ю.В., Норин В.А. – СПб.: Издательство «Лань» , 2019
2. Иванов И. А., Метрология, стандартизация, сертификация: учебник/ Иванов И. А., - Урушев С. В., Кононов Д. П., Воробьев А. А., Шадрина Н. Ю., Кондратенко В. Г. - СПб.: Издательство «Лань» , 2020

Дополнительные:

1. Кайнова В.Н., Метрология, стандартизация и сертификация: практикум/ Кайнова В.Н., Гребнева Т.Н., Тесленко Е.В., Куликова Е.А. - - СПб.: Издательство «Лань» , 2015

: http: //interstandart.ru›ms.htm.

5. ЛИСТ ЗМЕНЕНИЙ И ДОПОЛНЕНИЙ, ВНЕСЕННЫХ В МЕТОДИЧЕСКИЕ УКАЗАНИЯ

№ изменения, дата изменения, № страницы с изменением	
Было	Стало
Основание: Подпись лица, вносившего изменения	