Стандарты и спецификации в сфере информационной безопасности.

(Козырьков Игорь)

1.BS 7799-1:2005 — Британский стандарт BS 7799 первая часть. BS 7799 Part 1 — Code of Practice for Information Security Management (Практические правила управления информационной безопасностью) описывает 127 механизмов контроля, необходимых для построения *системы управления информационной безопасностью* (СУИБ) организации, определённых на основе лучших примеров мирового опыта (best practices) в данной области. Этот документ служит практическим руководством по созданию СУИБ

2.BS 7799-2:2005 — Британский стандарт BS 7799 вторая часть стандарта. BS 7799 Part 2 — Information Security management — specification for information security management systems (Спецификация системы управления информационной безопасностью) определяет спецификацию СУИБ. Вторая часть стандарта используется в качестве критериев при проведении официальной процедуры сертификации СУИБ организации.

3.BS 7799-3:2006 — Британский стандарт BS 7799 третья часть стандарта. Новый стандарт в области управления рисками информационной безопасности

4.ISO/IEC 17799:2005 — «Информационные технологии — Технологии безопасности — Практические правила менеджмента информационной безопасности». Международный стандарт, базирующийся на BS 7799-1:2005.

5.ISO/IEC 27001 — «Информационные технологии — Методы обеспечения безопасности — Системы управления информационной безопасностью — Требования». Международный стандарт, базирующийся на BS 7799-2:2005.

6.ISO/IEC 27002 — Сейчас: ISO/IEC 17799:2005. «Информационные технологии — Технологии безопасности — Практические правила менеджмента информационной безопасности». Дата выхода — 2007 год.

(Савостин Евгений)

1.ГОСТ 28195-89 - стандарт, устанавливающий критерии оценки качества программных средств.
2.ГОСТ Р ИСО/МЭК 12207-2010 (ISO/IES 12207:2008) - стандарт описывает процессы жизненного цикла ПО.

3.ГОСТ Р ИСО 9127-94 - стандарт описывает информацию по упаковке и документацию пользователя, которыми снабжаются потребительские программные пакеты.
4.ГОСТ 19.102-77 - стандарт устанавливает стадии разработки программ и программной документации для вычислительных машин, комплексов и систем.
5.ISO/IEC 27005 — Сейчас: BS 7799-3:2006 — Руководство по менеджменту рисков ИБ.

(Рудницкий Никита Российские и международные стандарты в области инженерии программных средств)

1. ***SO/IEC 14764:2006 «Разработка программного обеспечения. Процессы жизненного цикла программного обеспечения. Сопровождение»***.

Из-за ограничений в стоимости и сроках разработки в ПС нередко возникают ошибки в процессе эксплуатации. Часто приходится модернизировать ПС, чтобы удовлетворить изменившимся требованиям пользователя. Сопровождение ПС может в стоимостном отношении составлять наибольшую часть ЖЦ.Настоящий стандарт детализирует процесс сопровождения, описанный в ISO/IEC 12207. В стандарте также установлены определения различных типов сопровождения, приведены рекомендации по планированию и выполнению процесса сопровождения, контролю и надзору за ним, оценке и прекращению указанного процесса.

2. ***ISO/IEC 16085:2006 «Системы и разработка программного обеспечения. Процессы жизненного цикла. Управление рисками»***.

Настоящий стандарт устанавливает процесс менеджмента риска на различных стадиях ЖЦ ПС. Рекомендуется применять этот стандарт совместно с ISO/IEC 12207 и ISO/IEC 15288. Согласно этим стандартам менеджмент риска является одним из основных факторов, обеспечивающих успех организации при проектировании ПС.

3. ***ГОСТ 34.601-90 «Автоматизированные системы. Стадии создания»***.

Настоящий стандарт распространяется на автоматизированные системы (АС), используемые в различных видах деятельности (исследование, проектирование, управление и т. п.), включая их сочетания, создаваемые в организациях, объединениях и на предприятиях. Стандарт устанавливает стадии и этапы создания АС. Согласно ГОСТ 34.601-90, процесс создания АС представляет собой совокупность упорядоченных во времени,

взаимосвязанных, объединенных в стадии и этапы работ, выполнение которых необходимо и достаточно для создания АС, соответствующей заданным требованиям.Стадии и этапы создания АС выделяются как части процесса создания по соображениям рационального планирования и организации работ, заканчивающихся заданным результатом. Работы по развитию АС осуществляют по стадиям и этапам, применяемым для создания АС. Состав и правила выполнения работ на установленных настоящим стандартом стадиях и этапах определяют в соответствующей документации организаций, участвующих в создании конкретных видов АС.

4. ***ГОСТ 34.602-89 «Информационная технология. Комплекс стандартов на автоматизированные системы. Техническое задание на создание автоматизированной системы»*.**

Настоящий стандарт устанавливает состав, содержание, правила оформления документа «Техническое задание на создание системы». В стандарте присутствует образец первого и последнего листа данного документа.

5. ***ISO/IEC 25020:2007 «Разработка программного обеспечения. Требования к качеству и оценка качества программного продукта. Измерительная эталонная модель и руководство»*.**

Международный стандарт, устанавливающий требования к формированию метрики качества, которая строится на основе модели, определённой в стандартах ISO/IEC 2501N. Он также содержит информативные приложения, рассматривая следующие темы: выбор характеристик качества ПС и атрибутов качества, демонстрируя измерения оценок надежности и примерный формат для документирования мер качества ПС. Требования данного стандарта служат основанием для использования стандартов ISO/IEC 25030 и ISO/IEC 25040.

6. ***ISO/IEC 25041:2012 «Разработка систем и программ. Требования и оценивание качества систем и программ. Руководство по оцениванию для разработчиков, покупателей и независимых оценщиков»*** *.*

Международный стандарт (результат замены ISO/IEC 14598 3-5:1998-2000), определяющий структуру и содержание документации, которая будет использоваться при формирования модулей оценки. Эти оценочные модули содержат спецификацию модели качества (т.е. характеристики, подхарактеристики и атрибуты внешнего, внутреннего качества и качества в использовании), соответствующие данные и информацию о планируемом применении модели. Для каждого конкретного случая выбирается свой модуль

оценки, но в некоторых случаях может возникнуть необходимость в разработке нового модуля. Руководство по разработке нового модуля можно найти в настоящем стандарте.

7. ***ISO/IEC 25045:2012 «Разработка систем и программного обеспечения. Требования к качеству и оценка качества систем и программного обеспечения. Модуль оценки восстанавливаемости»***.

Международный стандарт, описывающий модуль для оценки характеристик восстановления. Он определяет внешние атрибуты качества для отказоустойчивости и восстанавливаемости для ПС. При измерении атрибутов, один или несколько ПС в процессе выполнения некоторых действий подвергают серии нарушений – например, оперативному закрытию процесса операционной системы или значительному увеличению пользователей в системе.