УДК 004.415

# СТАНДАРТЫ В ОБЛАСТИ КРИТИЧЕСКИХ ИНФОРМАЦИОННЫХ ТЕХНОЛОГИЙ И ПРОГРАММНОЙ ИНЖЕНЕРИИ: СИСТЕМАТИЗАЦИЯ, ПРОФИЛИРОВАНИЕ, ГАРМОНИЗАЦИЯ ТРЕБОВАНИЙ

*В.В. Скляр, канд. техн. наук*

*Харьковский филиал Государственного научно-технического центра ядерной и радиационной безопасности*

Проанализированы преимущества и недостатки применения стандартов в области критических информационных технологий. Предложена общая система классификационных признаков (таксономия) для систематизации стандартов в области критических приложений и таксономия стандартов по программной инженерии. Проанализированы результаты систематизации стандартов по программной инженерии. Разработана процедура формирования нормативных профилей на основе профилеобразующей базы.

* * *

Проаналізовано переваги та недоліки застосування стандартів в області критичних інформаційних технологій. Запропоновано загальну систему класифікаційних ознак (таксономія) для систематизації стандартів в області критичних додатків і таксономію стандартів з програмної інженерії. Проаналізовано результати систематизації стандартів з програмної інженерії. Розроблено процедуру формування нормативних профілів на основі профілеутворюючої бази.

* * *

Advantages and disadvantages of standards using in critical information technologies area are analyzed in the paper. General system of classification (taxonomy) for standards systematization in area of critical application and taxonomy for standards in area of software engineering are proposed. Results of standards systematization in area of software engineering are analyzed. Procedure of normative profile forming based on profile-formative base is elaborated.

## Введение

Бурное развитие науки и техники привело к тому, что рост технических возможностей превысил способность человечества к овладению этими новыми возможностями и их рациональному использованию. Не является исключением и программная инженерия. Постоянное совершенствование процессов создания программ пока не привело к созданию универсального метода, позволяющего в запланированные сроки создавать программные продукты заданного качества.

В то же время расширяется применение компьютерных систем управления (КСУ) в критических отраслях, т.е. в таких отраслях деятельности человека, негативные события в которых могут иметь критические последствия для жизни и здоровья людей, экологии или экономики. Однако внедрение КСУ может привести вместо ожидаемого снижения рисков (дефицитов безопасности) к возникновению новых. Так, известны случаи, когда КСУ и их программное обеспечение (ПО) служили причиной аварий космических аппаратов и ракетоносителей, приводили к облучению и гибели людей из-за неправильного управления радиологическим медицинским оборудованием, не говоря уже о повседневных финансовых потерях, связанных с отказами КСУ во всех областях человеческой деятельности.

Одной из основных проблем, возникающих при разработке ПО для КСУ, является сложность. Один разработчик практически не в состоянии охватить все аспекты большой системы, а привлечение дополнительных людских ресурсов порождает дополнительные коммуникационные проблемы.

Одним из способов борьбы со сложностью является накопление и передача опыта разработчиков и пользователей. Официальным аспектом этого процесса является стандартизация.

Выделяют следующие цели стандартизации [1]:

- обеспечение интерфейсов между разработчиками и пользователями продукта (коммуникативная функция);
- снижение трудоемкости, длительности, стоимости и улучшение других технико-

экономических показателей проектов;

- повышение качества разрабатываемых или применяемых покупных (COTS – Commercial Off The Shelf) компонентов при их разработке, эксплуатации и сопровождении;

- обеспечение возможности масштабировать конечный продукт по набору прикладных функций (расширение и интеграция);

- обеспечение переносимости программного продукта между разными операционными средами.

В то же самое время применение стандартов имеет следующие негативные последствия:

- существование большого количества стандартов, отсутствие четкой системы, наличие разных организаций, занимающихся стандартизацией в одной и той же сфере;

- неполное и неравномерное покрытие объектов стандартизации;

- «война стандартов», т.е. лоббирование интересов отдельных фирм в ущерб решению общих проблем стандартизации;

- регламентация в основном только наиболее простых объектов и массовых процессов;

- долгий срок разработки стандартов (три-пять лет), что приводит к их консерватизму и отставанию от практических потребностей.

Таким образом, будучи средством борьбы со сложностью, стандартизация сама вносит дополнительную сложность в процесс разработки ПО и КСУ, и данное противоречие требует разрешения.

Проблема может быть решена путем систематизации множества стандартов и их требований. Этому посвящены монографии [1–3]. Кроме того, различные подходы к разработке классификационных схем для стандартов в различных отраслях предложены в работах [4,5]. Перечень стандартов в области программной инженерии содержится, например, в монографии [1], в сборниках [6,7].

Однако, в перечисленных публикациях, во-первых, отсутствует полный перечень стандартов, а, во-вторых, не разработаны формальные процедуры, позволяющие автоматизировать процессы работы с текстами и перечнем стандартов при разработке ПО.

Целью данной статьи является разработка универсальной системы классификационных признаков (таксономии) для систематизации стандартов в области критических информационных технологий, а также разработка процедур гармонизации (сопоставления между собой) требований стандартов от разных разработчиков.

**Принципы построения нормативных профилей в области критических информационных технологий**

Для выработки подхода к решению сформулированной выше задачи использованы положения и определения стандарта ISO/IEC TR 10000-1:98 «Information technology – Framework and taxonomy of International Standardized Profiles – Part 1: General principles and documentation framework» (Основы и таксономия международных функциональных стандартов. Часть 1. Общие положения и основы документирования).

Профилем согласно ISO/IEC TR 10000-1 называется множество, состоящее из одного или нескольких базовых стандартов и/или международных функциональных стандартов, а также, при необходимости, из определений выбранных классов, соответствующих подмножеств, вариантов и параметров, определенных в данных стандартах, необходимых для выполнения конкретной функции.

Таким образом, под нормативным профилем понимается совокупность нескольких стандартов (или подмножество одного из них) с четко определенными и гармонизированными подмножествами обязательных и факультативных возможностей, предназначенная для реализации заданных функций [1].

Таксономия является классификационной схемой для однозначного определения типа профилей или набора профилей.

В настоящее время в мире существует ряд организаций, занимающихся стандартизацией [6,7]. Среди наиболее авторитетных следует назвать международные организации ISO (International Organization for Standardization – Международная организация по стандартизации, ИСО), IEC

(International Electrotechnical Commission – Международная электротехническая комиссия, МЭК), в области ядерной безопасности – IAEA (International Atomic Energy Agency – Международное агентство по атомной энергии, МАГАТЭ), а также американские IEEE (Institute of Electrical and Electronics Engineers – Институт инженеров по электротехнике и электронике), ANSI (American National Standardization Institute – Американский национальный институт стандартизации), которые, имея статус национальных, фактически имеют международное значение. Зачастую складывается такая ситуация, когда в одной области имеется несколько стандартов от разных организаций. Таким образом, весьма актуальной является задача систематизации функциональных (общетехнических, отраслевых) стандартов от разных организаций и формирование набора требований, содержащихся в разных документах, но необходимых для регламентации работы над определенным проектом (нормативных профилей [1,3]).

Основу нормативной базы, которая используется при разработке регулирующих требований к КСУ, составляют [5]:

- законы Украины и постановления Кабинета Министров, относящиеся к использованию критических технологий и к безопасности;
- нормы и правила по безопасности в отдельных отраслях и нормативные акты Регулирующих органов Украины;
- государственные стандарты, принятые Межгосударственным советом стран СНГ по стандартизации, метрологии и сертификации и действующие в Украине в статусе межгосударственных стандартов;
- государственные стандарты Украины и руководящие нормативные документы Госстандарта Украины;
- стандарты и руководства по безопасности, разработанные международными организациями (ИСО, МЭК, МАГАТЭ и др.);
- национальные стандарты США, России и других стран.

В табл. 1 предложена общая система классификационных признаков для стандартов и других нормативных документов в области критических приложений. Ячейка таблицы «ТАКСОНОМИЯ» предполагает детализацию классификационных признаков для конкретной прикладной области стандартизации.

Таким образом, задача стандартизация в области критических информационных технологий осложняется еще и тем, что кроме стандартов с требованиями к безопасности необходимо учитывать требования стандартов, отражающих общие положения, присущие применению некритических информационных технологий. Одной из областей, характеризующихся большим объемом стандартов различных организаций-разработчиков, является программная инженерия [3,8].

Таблица 1.

Система классификационных признаков (таксономия) для стандартов и нормативных документов (НД) в области критических приложений

| **Организация-разработчик** | **Национальная принадлежность** | **Уровень безопасности** | **Уровень НД** | **Дополнительные классификационные признаки** |
|---|---|---|---|---|
| ИСО | Международные | Общая | Законы и подзаконные акты | ТАКСОНОМИЯ |
| МЭК | Межгосударственные | Критический объект | Стандарты | |
| СЕНЕЛЕК | Национальные стандарты Украины | КСУ | НД по безопасности в отдельных отраслях | |
| Национальные и специализированные организации | Национальные стандарты других стран | Компоненты КСУ | Рекомендательные документы | |

**Построение таксономии стандартов в области программной инженерии**

В ходе анализа и отбора исходных данных использовался материал официальных Web-сайтов международных организаций: ISO – www.iso.ch; IEC – www.iec.ch; IEEE – www.ieee.org. Для анализа было отобрано 98 стандартов, регламентирующих разработку ПО.

Проведенный анализ показал, что наиболее развитую систему стандартов в области программной инженерии имеют ISO и IEEE. Что касается IEC, следует отметить, что в рамках этой структуры действует совместный с ISO технический комитет, занимающийся стандартизацией в области информационных технологий (ISO/IEC Joint Technical Committee for Information Technology – JTC1), который выпускает совместные НД (ISO/IEC). В состав этого комитета входит ряд подкомитетов, один из которых занимается непосредственно стандартизацией в области программной инженерии (JTC1/SC7 Software Engineering).

Таким образом, дальнейший анализ проводится для стандартов ISO и IEEE, причем большинство стандартов ISO разработаны совместно с IEC.

Каталог стандартов ISO имеет сложную многоуровневую иерархическую структуру и содержит 38 категорий. Для анализа была выбрана категория 35 «Information technology. Office machines», а из нее, в свою очередь, подкатегория 35.080 «Software development and system documentation». Данная группа насчитывает 60 стандартов. Большая их часть является совместной для ISO/IEC, хотя имеется несколько стандартов, действующих только в рамках ISO. Кроме того, часть стандартов представлена техническими отчетами (Technical Report), т.е. носят рекомендательный характер.

Каталог стандартов IEEE содержит 11 категорий (Application Areas; Circuits and Devices; Communication and Information; Computer Engineering; Control and Automation; Electromagnetics; General Interest; Instrumentation, Measurement and Testing; Interdisciplinary; Nuclear and Plasma Science; Power and Energy), которые, в свою очередь, делятся на ряд подкатегорий. Для анализа были отобраны две подкатегории (Software Design/Development; Software Quality and Management) из состава Computer Engineering. Данная группа насчитывает 38 стандартов. Следует отметить, что среди них имеются как непосредственно стандарты (Standard), так и руководства (Guide) и рекомендации (Recommended Practice).

Таксономию стандартов по программной инженерии предложено представлять в виде матрицы (табл. 2), столбцам которой соответствует уровень стандартов (системный или программный), а строкам – процессы ЖЦ ПО. Элементами матрицы являются названия (номера) стандартов, систематизированные по этим двум классификационным признакам. Следует отметить, что одному элементу матрицы может соответствовать несколько различных стандартов. Данный подход базируется на положениях стандарта IEEE 1002-1987 "IEEE Standard Taxonomy for Software Engineering Standards" (Стандартная таксономия для стандартов по программной инженерии).

Для формирования перечня процессов ЖЦ ПО был использован стандарт ISO/IEC 12207:1995 «Information technology – Software life cycle processes» (Процессы жизненного цикла программного обеспечения). Следует отметить, что второй стандарт принят в качестве национального стандарта Украины под номером ДСТУ 3918-1999. Исходный перечень процессов ЖЦ ПО был модифицирован в соответствии с номенклатурой имеющихся стандартов.

**Анализ результатов систематизации**

Проведенная классификация стандартов и нормативных документов (НД) позволила разделить все множество стандартов в соответствии с тремя классификационными признаками:

1) 17 процессов ЖЦ и три раздела (основы ЖЦ, поддержка ЖЦ, специальные процессы ЖЦ), в соответствии с которыми были сгруппированы эти процессы;

Таблица 2

Таксономия стандартов по программной инженерии

| Раздел процессов ЖЦ | Процесс ЖЦ |
|---|---|
| Основы жизненного цикла | Поставка и приобретение |
| | Анализ требований |
| | Проектирование |
| | Реализация (кодирование и тестирование) |
| | Интеграция системы |
| | Эксплуатация и сопровождение |
| Поддержка жизненного цикла | Документирование |
| | Конфигурационное управление |
| | Обеспечение качества |
| | Верификация и валидация |
| | Управление проектом |
| Специальные процессы жизненного цикла | Разработка терминологии |
| | Описание процессов жизненного цикла |
| | Спецификация данных и протоколов |
| | Измерение свойств и номенклатура |
| | Использование OTS и повторное использование |
| | Применение CASE-средств и формальных методов |

2) два уровня (системный и программный);

3) три организации-разработчика (ISO, ISO/IEC, IEEE).

Анализ распределения НД по разделам и процессам ЖЦ позволил сделать следующие выводы:

– наименьшее количество НД (12 или 13%) приходится на основы ЖЦ, которые фактически описывают основные фазы или этапы ЖЦ; небольшое количество НД объясняется тем, что в настоящее время структура ЖЦ уже четко определена, что отражается и на четкой структуре НД;

– несколько больше НД (22 или 23%) приходится на процессы поддержки ЖЦ; данный факт следует объяснить тем, что процессы поддержки ЖЦ ПО характеризуются большей сложностью и неопределенностью;

– подавляющее большинство НД (62 или 64%) приходится на специальные процессы ЖЦ; очевидно, что данный раздел определяет наиболее сложные процессы ЖЦ, которые, к тому же, обладают и наибольшей динамикой развития;

– распределение НД по конкретным процессам ЖЦ отражает основные тенденции распределения по разделам процессов ЖЦ, описанные выше;

– однозначно определены одним НД только два процесса ЖЦ: приобретение и интеграция;

– небольшим количеством НД (2-3) регламентированы все остальные процессы основ ЖЦ, а также конфигурационное управление, верификация и валидация, разработка терминологии;

– наибольшее число НД (25, более четверти всей нормативной базы), приходится на процесс измерения свойств ПО; очевидно, что данный процесс является наиболее сложным с теоретической точки зрения, и многообразие существующих НД отражает этот факт;

– значительное количество НД посвящено применение CASE-средств и формальных методов (15), а также использованию COTS и повторному использованию ПО (10).

Анализ распределения НД по организациям-разработчикам позволил сделать следующие выводы:

– наименьшее количество НД (7 или 7%) разработано ISO: по одному НД в области документирования, обеспечения качества, спецификаций данных и протоколов, а также четыре НД, посвященных формальным методам спецификаций; все НД (кроме НД по управлению качеством ISO 9000-3) были разработаны до 1990-х гг., а в настоящее время разработкой НД по программной инженерии в рамках ISO занимается совместный с IEC технический ко-

митет JTC1;

– более половины НД по программной инженерии (53 или 54%) разработаны совместно организациями ISO и IEC (JTC1);

– организацией IEEE разработано 38 НД, которые составляют 39% от общей нормативной базы;

– распределение НД различных организаций-разработчиков по разделам ЖЦ показывает, что НД IEEE составляют более развитую нормативную базу для процессов основ ЖЦ и их поддержки; НД ISO/IEC составляют подавляющее большинство для специальных процессов ЖЦ; анализ распределения НД различных организаций-разработчиков по процессам ЖЦ подтвердил данную тенденцию;

– четкое разграничение сферы деятельности двух основных организаций разработчиков (IEEE и JTC1) имеет место для следующих процессов ЖЦ: поставка и приобретение, реализация, верификация и валидация (все IEEE), интеграция, спецификация данных и протоколов (все – ISO/IEC); для остальных процессов ЖЦ параллельно существуют НД разных организаций;

– факт существования нескольких НД для одного и того же процесса ЖЦ придает актуальность задаче формирования профилей, а также задаче гармонизации требований НД, разработанных разными организациями; решение этой задачи возможно путем детального анализа (препарирования и сопоставления) требований НД.

Анализ распределения НД по уровням (системный и программный) позволил сделать следующие выводы:

– системный уровень регламентируют 23 НД, которые составляют 23% от общей нормативной базы; системный уровень регламентируют 75 НД, которые составляют 77% от общей нормативной базы;

– большинство НД системного уровня (19) относятся к разделу специальных процессов ЖЦ;

– из специфики процессов ЖЦ ПО следует, что НД программного уровня не существует для процессов интеграции системы и спецификации данных и протоколов; НД системного уровня не существует для описания процессов жизненного цикла, всех процессов основ ЖЦ, за исключением проектирования и интеграции, а также всех процессов поддержки ЖЦ, за исключением документирования;

– «пробелы» в нормативной базе для системного уровня означают, что для полного формирования нормативного профиля следует использовать НД для той прикладной области, в которой планируется применять рассматриваемую КС.

Следует отметить, что кроме данного подхода к систематизации стандартов существуют, например, уровневые диаграммы (Layer Diagrams), предложенные Джеймсом Муром в работе [2]. Стандарты по программной инженерии предлагается делить на шесть уровней (от более общих к более специфическим стандартам):

– терминология (стандарты, описывающие термины и словари);

– общее руководство (руководства, предваряющие группу стандартов);

– принципы (стандарты, описывающие принципы);

– элементарные стандарты (типичные базовые стандарты);

– прикладные руководства (поддерживают использование стандартов);

– методики (стандарты, описывающие методы или методики, которые дополняют требования или руководства группы стандартов).

Проведенный анализ показал, что данная классификационная система позволяет установить общность стандартов, но при этом не характеризует прикладную область их использования.

### Процедуры формирования профилеобразующей базы и нормативного профиля

При анализе требований стандартов, а также при сертификации ПО относительно соответствия требованиям стандартов необходимо проводить сравнительный анализ требований различных стандартов, относящихся к одному и тому же процессу ЖЦ.

Описанная выше таксономия была применена для систематизации стандартов в целом. Однако, кроме этого, возникает задача систематизации для более низкого уровня – для уровня требований, содержащихся в стандарте. При этом может оказаться, что для детализации одного требования, содержащегося в базовом стандарте, может быть разработано несколько других стандартов. Таким образом, понятие таксономии следует применять не только для стандартов в целом, но и для требований, причем эти два уровня тесно связаны нормативным профилем, так как в профиль может войти только часть какого-либо стандарта (подмножество требований).

Для решения задачи сравнительного анализа требований были предложены процедуры и формирования профилеобразующей базы (рис. 1) и гармонизации (рис. 2). Для описания процедур введем ряд терминов:

Профилеобразующая база – множество, состоящее из одного или нескольких стандартов, служащее основой для формирования нормативных профилей.

Профилеобразующий стандарт – стандарт, структура которого выбрана в качестве таксономии для множества стандартов и/или требований.

Гармонизация – сопоставление относительно непротиворечивости требований международных и/или национальных стандартов, разработанных разными организациями и соответствующих одному нормативному профилю.

Препарирование – анализ стандарта в целях его структурирования в соответствии со структурой нормативного профиля.

## Заключение

В результате предложенной процедуры систематизации стандарт однозначно позиционируется в матрице классификационных признаков. Данное свойство классификационной матрицы позволяет построить реляционную базу данных стандартов. Такая база данных, в свою очередь, может служить основой для инструментального средства, выполняющего функции анализа и структурирования требований (препарирования), формирования нормативных профилей, гармонизации нормативных профилей для стандартов, разработанных различными организациями.

## Литература

1. Липаев В.В. Обеспечение качества программных средств. Методы и стандарты.– М.: СИНТЕГ, 2001.– 380 с.

2. Moore J. Software Engineering Standards. A User's Map.– Los Alamos, CA, USA: IEEE Computer Society, 1998.

3. Конорев Б.М. и др. Нормативная база программной инженерии в разработке систем с интенсивным использованием программного обеспечения.– Х.: НАКУ «ХАИ», 2001.– 162 с.

4. Johnson G. Comparison of IEC and IEEE Standards for Computer-Based Control Systems Important to Safety // Proceedings of CNRA/CSNI Workshop on Licensing and Operating Experience of Computer-based I&C Systems.– Hluboka nad Vltavou (Czech Republic).– 2001.– P. 109-115.

5. Ястребенецкий М.А., Розен Ю.В., Васильченко В.Н. Нормирование и оценка безопасности информационных и управляющих систем АЭС (2): Принципы нормирования // Ядерная и радиационная безопасность.- 2001.– Т. 4.– № 1.– С. 16-23.

6. Сертификация продукции. Международные стандарты и руководства ИСО/МЭК в области сертификации и управления качеством.– М.: Изд-во стандартов, 1990.

7. IEEE Standards Collection Software Engineering.– New York, NY, USA: IEEE Inc., 1994.

8. Харченко В.С., Ястребенецкий М.А., Скляр В.В. Новые информационные технологии и безопасность информационно-управляющих систем АЭС // Ядерная и радиационная безопасность.- 2003.– Т. 6.– № 2.– С. 19-28.

*Поступила в редакцию 15.01.03*

**Рецензент:** д-р техн. наук, профессор Краснобаев Виктор Анатольевич, Харьковский государственный технический университет сельского хозяйства, г. Харьков.

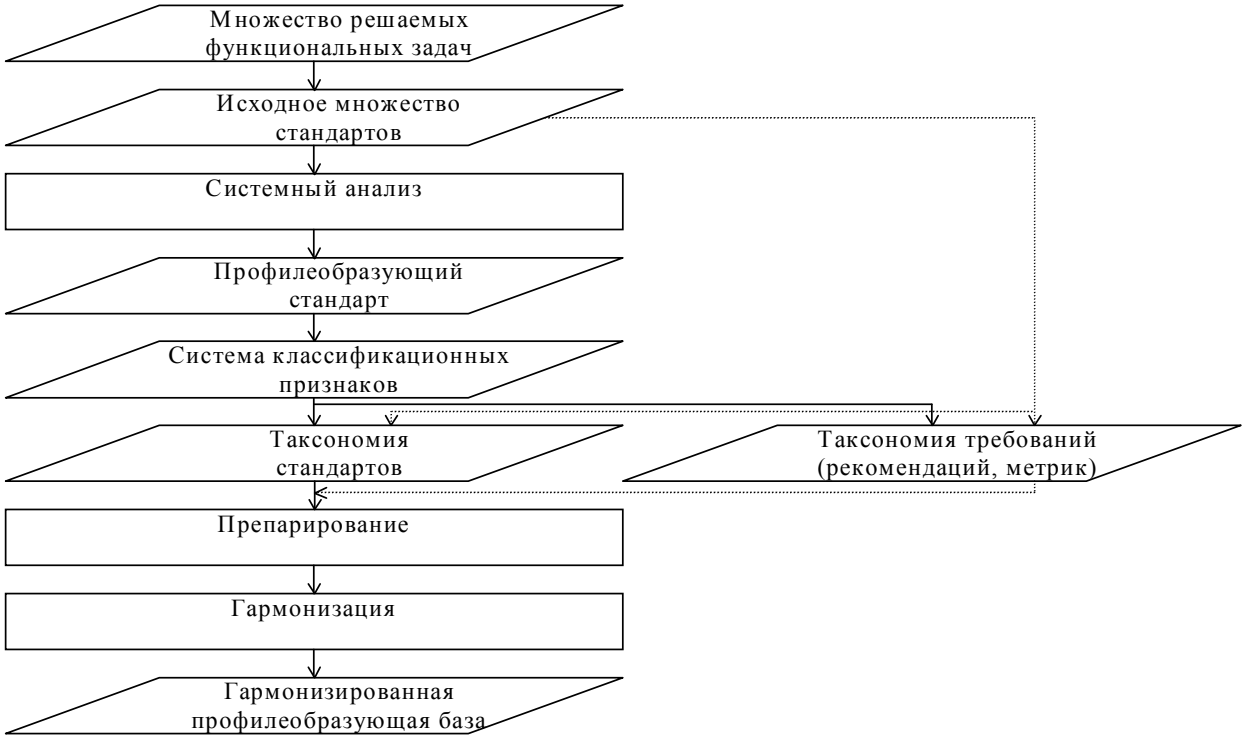


Рис. 1. Процедура формирования профилеобразующей базы

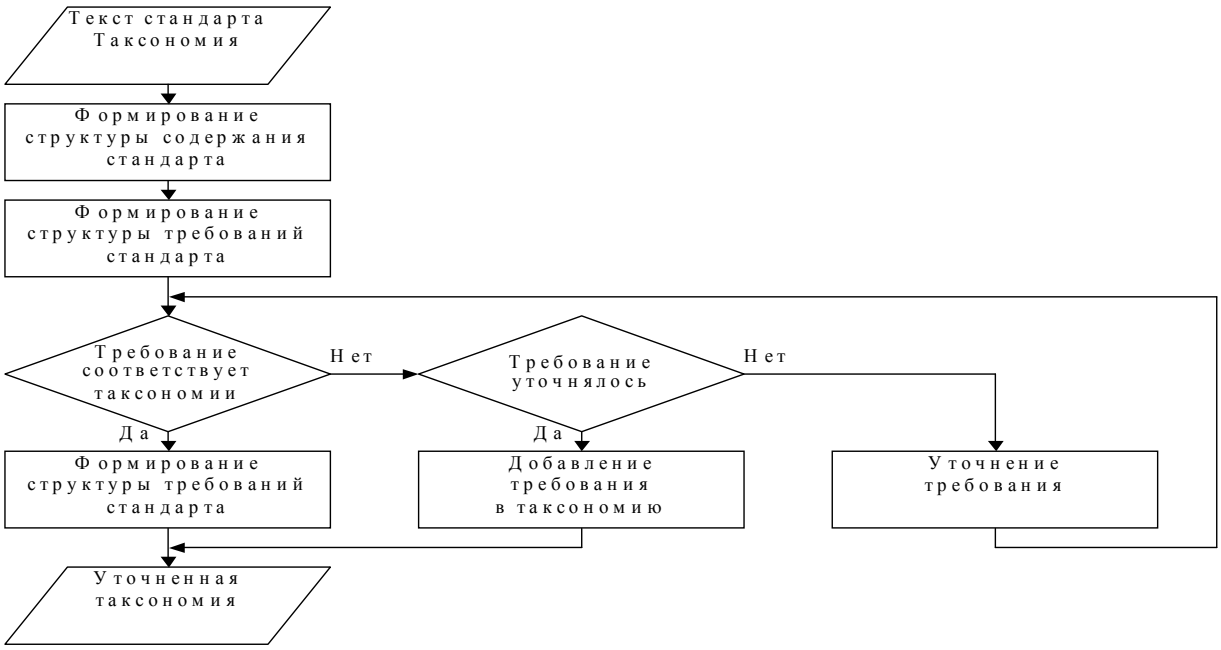


Рис. 2. Процедура гармонизации требований стандартов