УДК 004.9.615.12

А. А. ФЕДОСЕЕВА

Национальный фармацевтический университет, Украина

ОЦЕНКА ТРЕБОВАНИЙ К ПРОГРАММНОМУ ОБЕСПЕЧЕНИЮ ФАРМАЦЕВТИЧЕСКОГО ПРЕДПРИЯТИЯ НА ОСНОВЕ SAFETY-CASE МЕТОДОЛОГИИ

Рассмотрены требования к ПО на фармацевтическом предприятии: к структуре ПО и его элементам, к процессу разработки ПО, к валидации, верификации, диагностированию, а также к защите данных и обеспечению доступа к данным; проведен анализ существующих подходов к оценке качества и безопасности ИУСКП; предложена иерархическая модель требований к ПО; проведен анализ характеристик ПО и выявлены метрики, позволяющие оценить требования к нему: безопасность, эффективность, продуктивность, функциональность, удовлетворимость потребностей; предложена модель качества в использовании для ПО на ФП.

Ключевые слова: *программное обеспечение, Safety-Case, метрика, безопасность, информационно-управляющая система критического применения, стандарт безопасности, дерево требований, фармацевтическое предприятие.*

Введение

Современное общество предъявляет высокие требования к обеспечению безопасности объектов фармацевтической промышленности [1,2], включая и информационные управляющие системы (ИУС) на производственных предприятиях. Особое внимание при этом должно обеспечению безопасности работы УИС в критических состояниях (условиях). Для критических областей, таких как фармацевтическая отрасль, актуальной задачей является разработка моделей, методов и методик, а также инструментальных средств оценки качества и безопасности функционирования ИУС критического применения (ИУС КП), которые в настоящее время отсутствуют.

Для оценки качества и безопасности ИУСКП на ФП целесообразно использование подхода, который основан на методологии Safety-Case, которая была успешно реализована [3].

Разработка требований качества и безопасности к ПО на ФП необходима как для улучшения существующих ИУСКП, так и создания новых ИУСКП на ФП.

1. Постановка задачи

В рамках производственных спецификаций на ФП выдвигаются требования, которые обеспечивают функции ИУСКП на производстве и которые не включены в требования GAMP [1].

В рамках данной работы предложена модель требований к ПО на ФП (рис. 1), которая позволяет учесть как общие требования к ПО производственного предприятия, так и специфические

Предлагаемая модель позволяет рассматривать требования к качеству ПО на ФП с более общих позиций, нежели предусмотрено в стандартах [4] и [5] и требованиях [2].

Выбор Safety-Case методологии обусловлен тем, что:

- в настоящее время составление Safety-Case-документов является требованием таких международных стандартов по безопасности (например, IEC 1508, Def Stan, EN 292 Machinery Directive и др.);

- данная методика позволяет построить убедительное доказательство безопасности системы во времени [6].

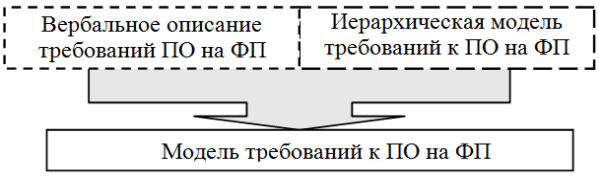

Рис. 1. Структура модели

План создания Safety-Case разрабатывается в самом начале оценки качества и безопасности ИУСКП, поскольку необходимо использование собранных доказательств на различных этапах ее проектирования. Чем выше требования к безопасности ИУСКП, тем выше необходимый уровень детализации требований к ПО на ФП.

2. Вербальное описание требований к ПО на ФП

Сформулируем вербально основные требования к ПО на ФП.

I. Требования к структуре ПО и его элементам

1.1. ПО должно соответствовать требованиям GMP и GAMP, быть достаточным для выполнения

всех необходимых функций.

1.2. ПО должно обеспечивать проведение провокационных испытаний (challenge tests) – условий, которые охватывают верхний и нижний пределы параметров стадий технологического процесса производства лекарственных препаратов.

1.3. ПО должно иметь модульную структуру.

1.3.1. Каждый модуль должен решать определенную задачу; быть легко изменяем и тестируем; иметь ограниченное количество операторов в листинге; должен быть совместим с другими модулями в рамках ИУС.

1.4. Должна существовать возможность использования ранее разработанного ПО с условием проведения его оценки для существующей ИУС.

1.4.1. Оценка ПО должна включать в себя анализ результатов работы ранее разработанного ПО;

1.4.2. Оценка ПО должна включать в себя принятие решения относительно возможности использования ранее разработанного ПО.

1.4.3. Оценка ПО должна включать в себя проверку соответствия функций, процедур и характеристик ранее разработанного ПО существующим на момент его модификации отраслевым спецификациям и требованиям GAMP и GMP.

1.4.4. Оценка ПО должна включать в себя внесение необходимых изменений в ранее разработанное ПО.

1.5. ПО для критических стадий и операций технологического процесса производства лекарственных препаратов должно разрабатываться отдельно, использование прерываний в ходе выполнения таких операций должно быть строго запрещено

1.6. Согласно директиве ЕС («Об установлении основных принципов и правил GMP лекарственных средств для человека») от 13.06.91 необходимо включать ревалидацию в разрабатываемое ПО.

1.7. ПО должно включать валидацию – документированные доказательства того, что система работает так, как должна работать.

1.8. Должны использоваться встроенные программы (подпрограммы) проверки правильности вводимых и выводимых данных.

1.9. В ПО должна быть предусмотрена возможность выдачи разрешений на реализацию серий ЛП для продажи.

II. Требования к процессу разработки ПО

2.1. Проектируемое ПО должно соответствовать таким критериям качества, как: надежность, изменяемость, корректность, простота интерфейса пользователя, а также стандартам качества предметной области.

2.2. Каждая стадия процесса разработки ПО должна быть строго и подробно документирована. Необходимо наличие подробного описания эксплуатации ПО.

2.3. Должны быть соблюдены технические инструкции – описание различных стадий технологического процесса и спецификации на исходное сырье и материалы.

2.4.-2.5. При использовании автоматизированных инструментальных средств разработки должны быть приведены обоснования их выбора; при использовании служебного ПО необходима его верификация по таким же критериям, как и разрабатываемое ПО.

2.6. На всех этапах разработки ПО необходимо использовать формальные математические методы, которые основаны на строгом математическом описании различных постановок задач.

2.6.1. Формальные математические методы применяются для разработки формализованных спецификаций ПО; для математического доказательства соответствия проектируемого ПО формализованным спецификациям и требованиям стандартов предметной области; для анализа синтаксической и семантической корректности ПО; для проведения тестовых проверок выполнения функциональных требований к ПО.

2.7. Необходимо избегать использования сложных программных реализаций: конструкций, приемов и методов программирования.

2.7.1.-2.7.4. Предпочтительно использование подпрограмм, унифицированных переменных, массивов заранее определенной размерности, стандартных процедур и функций.

2.8. Необходимо создание в проектируемом ПО возможности полного учета всех вводов данных и вносимых изменений – «проверка следа».

III.Требования к валидации

3.1. ПО, используемое при валидации, не должно приводить к снижению качества ЛС или влиять на обеспечение их качества.

3.2. ПО, используемое для валидации, должно содержать протокол валидации и отчет о валидации.

3.3. ПО, используемое в технологическом процессе производства ЛП, должно охватывать процесс ревалидации для критических стадий производства.

3.4. Каждая существенная модификация должна быть валидирована, что должно быть отражено в ПО.

IV.Требования к обеспечению доступа к данным

4.1. Ввод данных в систему должен быть разрешен только уполномоченным лицам.

4.2. Должны быть предусмотрены методики по предоставлению доступа, изменению или аннуляции уполномоченных лиц.

4.3.-4.4. Любое изменение ввода критических данных, например, таких как масса или номер серии ингредиента, должно быть санкционировано с указанием причины их модификации; в случае привлечения сторонних организаций для обеспечения компьютерного обслуживания необходимо иметь официальное соглашение о сотрудничестве с определением уровня доступа.

4.5. Выдача разрешений на реализацию серий ЛС на продажу должна осуществляться только уполномоченному лицу.

V. Требования к защите данных

5.1. ПО должно предусматривать защиту от отказов (сбоев) технических средств.

5.1.1.Требуется определить методики, которыми необходимо пользоваться при поломке или сбое системы. Они должны быть валидированы; данные должны быть защищены электронными или техническими средствами.

5.3. Необходимо обеспечивать защиту от несанкционированного доступа с помощью систем паролей, процедур цифровой подписей, алгоритмов шифрования и других методов защиты.

5.4. Должна существовать методика анализа и записи ошибок.

5.5. Все выявленные повреждения ПО или технических средств должны быть запротоколированы, как и действия по их устранению.

5.6. Необходимо создавать запасные копии данных через постоянные периоды времени.

5.7. Должен быть предусмотрен механизм использования альтернативных технических средств в случае отказа (поломки) существующих.

5.8. Хранимые данные необходимо проверять на сохранность, правильность и доступность.

5.9. Необходимо обеспечить защиту от вирусов и программных кодов, которые не предусмотрены отраслевыми спецификациями.

VI.Требования к диагностированию ПО

6.1. ПО должно осуществлять непрерывный автоматический контроль технического состояния ИУС технологического процесса производства ЛП.

6.2. -6.3. ПО должно обеспечивать техническое диагностирование ИУС, а также самодиагностирование с использованием различных методов; возможность проведения периодических проверок эксплуатации ИСУ.

6.4. Должна существовать возможность хранения и отображения данных о результатах диагностирования, самодиагностирования и проверок.

VII. Требования к верификации ПО

7.1. Верификацию необходимо проводить после каждого этапа разработки ПО.

7.2. Верификация должна быть полностью завершена к моменту сдачи ПО в эксплуатацию.

7.3. В ходе верификации необходимо определить источники отказов.

7.3.1. Отказов по общей причине.

7.3.2. По причине дефектов.

7.3.3. Определить последствия проявления дефектов в ПО.

7.4. Для ранее разработанного ПО возможна частичная верификация, которая затрагивающая только внесенные в ПО изменения.

7.5. При использовании программных модулей, которые требуют конфигурирования, необходимо предусмотреть верификацию модифицируемых программных модулей.

7.6. Перед началом верификации необходимо разработать ее план.

7.6.1. необходимо выбрать стратегию верификации.

7.6.2. Определить порядок верификации.

7.6.3. Выбрать методы и средства для верификации.

7.6.4. Определить порядок документирования действий по верификации.

7.7. Необходимо создание отчета по верификации.

7.7.1. Перечень входных и выходных параметров верификации.

7.7.2. Полученные результаты испытаний и их оценка.

7.7.3. Перечень обнаруженных неполадок ПО.

7.7.4. Сделанные выводы по результатам обнаруженных неполадок.

7.7.5. Необходимые мероприятия по устранению неполадок ПО.

7.8. Документация по верификации ПО должна быть изложена языком, понятным для специалистов, которые не участвовали в процессе верификации.

3. Иерархическая модель требований к ПО на ФП

Требования к ПО на ФП можно представить в виде иерархической многоуровневой модели (рис. 2). Каждый уровень представляет собой последовательную детализацию требований к ПО на ФП. Вершины, отмеченные цветом, определяют специфические отраслевые требования, присущие лишь фармации.

4. Модель качества в использовании для ПО на ФП

На основании иерархической модели построена модель качества в использовании ПО на ФП.

В данной модели выделены характеристики ПО и соответствующие им метрики [7], позволяющие формализовать и впоследствии их оценить:

1) безопасность (Security):

– контрольная оценка после каждой технологической операции;

– контрольная оценка после каждой технологической стадии;

– риск повреждения данных;

– риск ошибки в спецификациях на исходное сырье и материалы;

– контрольные параметры challenge tests;

– количество отказов ПО по причине дефектов.

2) эффективность (Efficiency):

– процент реализованных задач пользователя;

– процент пользователей, успешно завершивших задачу за единицу времени;

– среднее количество успешно пройденных технологических операций за единицу времени;

– среднее число не успешных постстадийных контрольных проверок;

– процент успешных валидационных и ревалидационных протоколов.

3) продуктивность (Productivity):

– количество технологических операций, выполненных за единицу времени;

– частота использования спецификаций;

– оптимальное время завершения технологической операции;

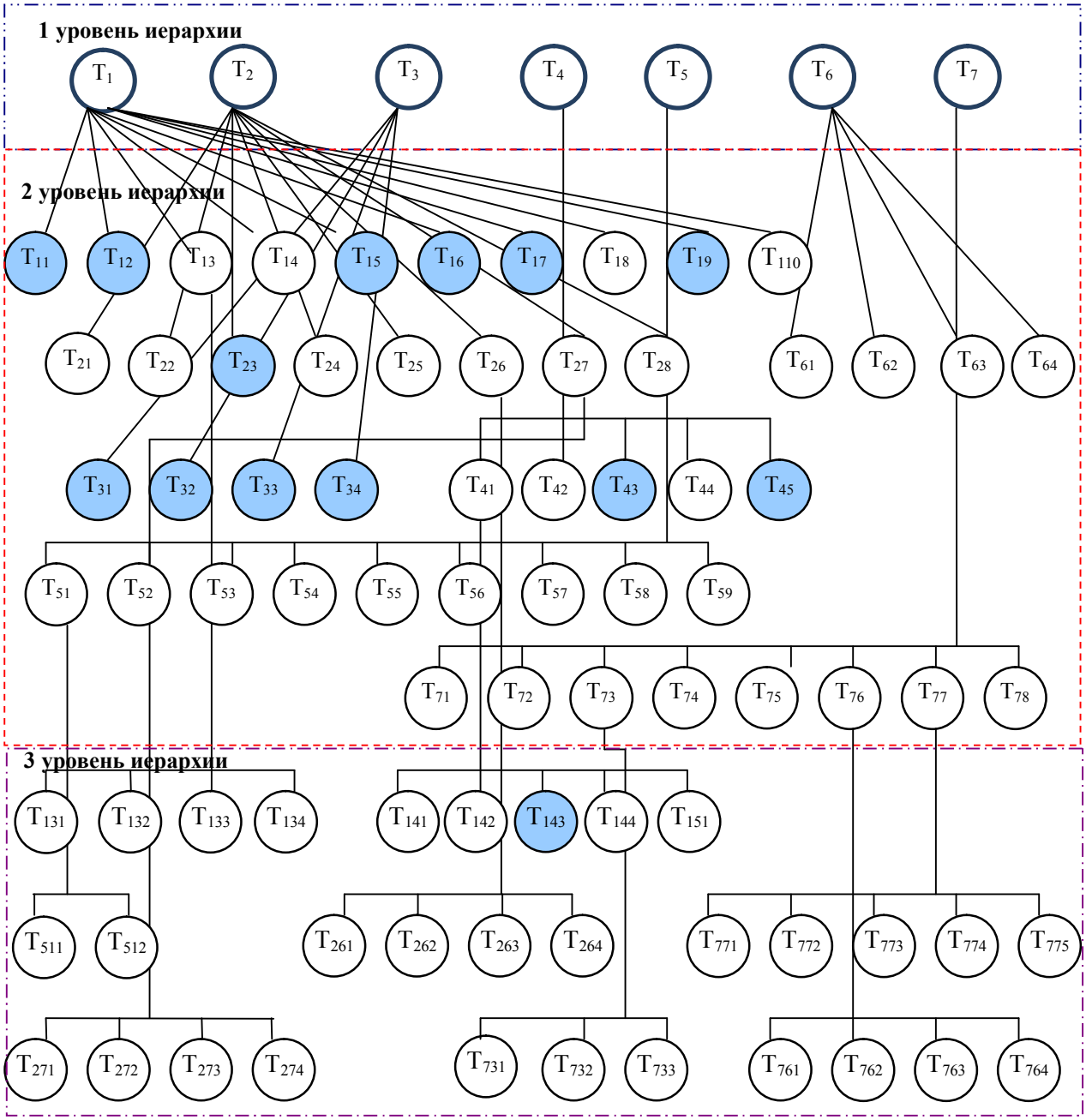

Рис. 2. Иерархическая модель требований к ПО на ФП

– оптимальное время завершения технологической стадии;

4) удовлетворимость потребностей пользователя (Usability);

– степень загрузки системы во времени;

– соотношение между «довольными» и «не довольными» пользователями;

– частота жалоб пользователей;

– рейтинговая оценка функциональности ПО;

– рейтинговая оценка полезности ПО.

5) функциональность (Functionality):

– количество используемых функций;

– количество используемых команд.

При выборе метрик учитывались цель их использования, которые были определены в вербальном представлении требований к ПО на ФП.

Количественные характеристики представленных метрик могут быть использованы для оценки качества и безопасности ПО на ФП.

Заключение

Построение иерархической модели к ПО на ФП позволяет выделить показатели качества, распределенные по иерархическому принципу. Иерархичность позволяет сформировать интегральный показатель, объединяющий в себе свойства всех других уровней. Метрики, соответствующие показателям третьего уровня иерархической модели, можно измерить, формализовать с целью их последующей оценки.

Таким образом, контенты каждой компоненты представленной модели требований к ПО на ФП в своей совокупности удовлетворяют как специфическим отраслевым требованиям GAMP, что отражается в нормативной документации ФП, так и общие требования к ПО ИУСКП.

Литература

1. GAMP Guide for Validation of automated systems [Электронный ресурс]. – Режим доступа: http://gartner.com.

2. International Organization for Standardization [Электронный ресурс]. – Режим доступа: http://www.iso.org/iso/home.html.

3. Case-оценка критических программных систем [Текст]. В 3 т. Т.3. Безопасность / В. С. Харченко, Е. И. Неткачева, А. А. Орехова, О. М. Тарасюк / под ред. В. С. Харченко. – Х. : Нац. аэрокосм. ун-т «ХАИ», 2012. – 301 с.

4. 1061-1998 IEEE Standard for Software Quality Metrics Methodology [Электронный ресурс]. – Режим доступа: http://www.iso.org/iso/catalogue_detail.htm?csnumber=20115.

5. ISO 8402:1994 Quality management and quality assurance [Text].

6. Dale, C. Safety-Critical Systems: Problems, Process and Practice [Text] / C. Dale, T. Anderson. – Springer, 2009. – 24 p.

7. ISO/IEC 25010:2011 Systems and software engineering - Systems and software Quality Requirements and Evaluation (SQuaRE) - System and software quality models [Text].

Поступила в редакцию 23.02.2014, рассмотрена на редколлегии 25.03.2014

Рецензент: д-р физ.-мат. наук, проф. И. К. Кириченко, Украинская инженерно-педагогическая академия, Харьков, Украина.

ОЦІНКА ВИМОГ ДО ПРОГРАМНОГО ЗАБЕЗПЕЧЕННЯ ФАРМАЦЕВТИЧНОГО ПІДПРИЄМСТВА НА ОСНОВІ SAFETY-CASE МЕТОДОЛОГІЇ

А. О. Федосєєва

Розглянуті вимоги до ПЗ на фармацевтичному підприємстві: до структури ПЗ та його елементам, до процесу розробки ПЗ, до валідації, верифікації, діагностиці, а також до захисту даних та забезпечення доступу до даних; проведений аналіз існуючих підходів до оцінки якості та безпеки ІУСКЗ; запропонована ієрархічна модель вимог до ПЗ; проведений аналіз характеристик ПЗ та виявлені метрики, які дозволяють оцінити вимоги до нього: безпеку, ефективність, продуктивність, функціональність, удовлетворимість потреб; запропонована модель якості в використанні для ПЗ на ФП.

Ключові слова*:* програмне забезпечення, Safety-Case, метрика, безпека, інформаційно-управляюча система критичного застосування, стандарт безпеки, дерево вимог, фармацевтичне підприємство.

ASSESSMENT REQUIREMENTS TO THE SOFTWARE FOR THE PHARMACEUTICAL ENTERPRISE BASED SAFETY-CASE METODOLOGY

A. A. Fedoseeva

Consider the requirements to the software in the pharmaceutical enterprise: to the software structure and its elements, to the development software process, to the validation, verification, diagnostics, data protection, data access; analysis the existing approaches to the assessment requirements and security of the ICSCU; the hierarchical model of the requirements to the pharmaceutical enterprise is proposed; the metrics, which could allow us to estimate requirements to the software are presented: efficiency, productivity, functionality, usability; the model of quality in use for the software in the pharmaceutical enterprise is proposed.

Key words: software, Safety-Case, metric, security, information control system for critical use, security standard, tree of requirements, pharmaceutical enterprise.

Федосеева Алина Александровна – ведущий специалист КЦ Национального фармацевтического университета, Харьков, Украина, e-mail: fedosaa@ukr.net.