

выполнить контрольную прямо у себя в телефоне. В свою очередь, приложение позволит автоматизировать проверку тестовых элементов контрольной. Преподаватель же избавляется от собираний листочков, получает в своём личном кабинете приложения уже проверенные тестовые задания и просматривает удобную статистику ответов для анализа труднодоступных вопросов.

Анализируя предметную область автоматизации тестирования средствами мобильных систем, была поставлена задача спроектировать и реализовать мобильное приложение для упрощения процесса тестирования и анкетирования среди студентов ВУЗов.

Система должна реализовывать следующие компоненты:

- Создание тестовых и контрольных работ преподавателем по заданной теме.
- Выполнение тестовых заданий студентами, предварительно зарегистрированными в системе.
- Просмотр итоговых результатов со статистикой для анализа пробелов в материале и знаниях студентов преподавателем.
- Возможность скачивания материалов для самостоятельного изучения или повторения студентами.
- Возможность просмотра оценок в текущем семестре за практические и лабораторные работы.

Разработанное приложение даст возможность оптимизировать процесс обучения, связанный с практическими работами и контролем знаний, позволит студентам избавиться от необходимости приносить ноутбуки вместе с книгами и конспектами. Вся необходимая информация и средства будут всегда вместе с ними. Кроме того, для преподавателей снижается нагрузка, которая в дальнейшем может быть распределена на актуализацию и структуризацию преподаваемого материала.

Список использованных источников:

1. Данилова, Г. В. Программное средство управления формированием IT-компетенций / Г. В. Данилова // Дистанционное обучение – образовательная среда XXI века : материалы IX международной научно-методической конференции (Минск, 3-4 декабря 2015 года). – Минск : БГУИР, 2015. – С. 300 - 301.

СИСТЕМА КОНТРОЛЯ И ОЦЕНКИ СОСТОЯНИЯ ПРОЦЕССА РАЗРАБОТКИ КОМПЛЕКСНЫХ ПРОГРАММНЫХ СРЕДСТВ ДЛЯ ТЕЛЕКОММУНИКАЦИОННОЙ ОТРАСЛИ

*Белорусский государственный университет информатики и радиоэлектроники
г. Минск, Республика Беларусь*

Кулаковский С.А.

Бранцевич П.Ю. – к.т.н., доцент

Показателем успешности реализации проекта является достижение поставленных перед проектом целей в рамках заданных ограничений по финансовым, материальным, человеческим и временным ресурсам. Наличие четкой системы организации и контроля выполнения проекта является ключевым аспектом его успешного завершения, особенно в высокотехнологичных, инновационных и динамичных отраслях, к которым относятся телекоммуникации. Наряду с другими этапами жизненного цикла проекта, особую важность представляет организация процесса разработки программного обеспечения и контроль состояния данного процесса, позволяющего заблаговременно внести необходимые коррективы и принять своевременные управленческие решения.

Телекоммуникационная отрасль на современном этапе развития представляет собой реализацию взаимодействия целого ряда аппаратно-программных комплексов на базе широкого стека информационных технологий, включающего виртуализацию, использование облачных решений, микросервисы, организацию межконтинентальных и космических каналов связи. Кроме инфраструктурных процессов, перед поставщиками телекоммуникационных услуг стоят задачи обработки, хранения и анализа огромных объемов данных, реализации внешних и внутренних информационных ресурсов, направленных на обеспечение бесперебойного доступа миллионов пользователей к предоставляемым сервисам. Некоммерческая ассоциация TMForum (TeleManagementForum) стандартизирует отрасль посредством разработки рекомендаций, описывающих концепции построения отраслевого программного обеспечения (описание интеграционных интерфейсов, моделей данных) [2]. Единая терминология, наличие списка бизнес-процессов и референтная карта приложений с описанием основных функций, позволяют уже на ранних этапах сформировать набор высокоуровневых требований и применять каскадную модель разработки программного обеспечения для реализации проекта. Типизация имплементационных задач позволяет поставщику нарабатывать необходимую экспертизу, продуктивизировать проектное решение и обеспечить необходимую точность экспертной оценки планируемых работ в каждом из телекоммуникационных доменов.

Система контроля и оценки состояния процесса разработки является механизмом количественной оценки, которая позволяет в любой момент времени оценить ключевые показатели процесса разработки, и на основании полученной информации принять необходимые управленческие решения. К таким решениям относятся: изменение состава команды разработки, переоценка сроков реализации проекта, оценка эффективности использования проектных ресурсов и их достаточности для успешного завершения проекта. Реализация основывается на адаптации ряда существующих подходов и методик, которая позволяет повысить точность проводимой оценки.

Для оценки трудоёмкости планируемого объёма работ применяется метод WBS (WorkBreakDownStructure) – иерархическая декомпозиция всего объёма работ до уровня, на котором задача может быть оценена и спланирована [1]. При проведении иерархического разбиения работ используется группировка задач по логическим доменам, где требуется привлечение разработчиков с однородным уровнем экспертизы и схожих технических навыков с учётом рекомендаций консорциума TMForum.

Формирование и учёт состава команды разработки происходит на основании ресурсного плана проекта, учитывающего не только доступность каждого ресурса (разработчика) с учётом выходных, праздничных дней, отпусков, но, также, и определённые показатели, характеризующие производительность и вовлечённость каждого разработчика:

Вовлечённость – характеристика, определяющая степень привлечения разработчика непосредственно к написанию программного кода. Разработчик может частично привлекаться на проект либо решать задачи в нескольких логических доменах, либо только частично заниматься непосредственно разработкой;

Производительность – коэффициент, определяющий способность разработчика решать задачи относительно оценки, определённой техническим лидером. Определяется на основании опыта разработчика в конкретном домене и в ходе проекта корректируется на основании накопленной статистики решения проектных задач.

Для оценки текущего состояния процесса разработки используется расширение метода освоенного объёма (EVT – EarnedValueTechnique) [1]. В разрезе количества задач и их трудоёмкости с учётом реализованного объёма работ определяется текущий статус процесса разработки в любой момент времени. На основании известных характеристик команды разработки и накопленных статистических данных производится расчёт планируемых дат окончания запланированных работ.

Система контроля и оценки состояния процесса разработки использует адаптацию каскадной модели разработки ПО, совмещая фазы разработки и тестирования. Привлечение команды тестирования для верификации реализованных функций на этапе разработки позволяет обнаружить большую часть дефектов на более ранних этапах. Введение количественного соотношения «входящих» задач (обнаруженные дефекты, улучшения либо необходимые дополнительные изменения) к «исходящим» задачам с учётом основного объёма работ и характеристик команды разработки, позволяет на базе экстраполяции оценить ожидаемую дату завершения работ и потенциальный сдвиг сроков разработки.

Список использованных источников:

1. Руководство к своду знаний по управлению проектами (Руководство РМВОК). – М.: Олимп-Бизнес, 2018 – 590с.
2. TM Forum. [Electronic resource] - <https://www.tmforum.org/>. Dateofaccess: 21.03.2018

АЛГОРИТМ DESX КАК СРЕДСТВО ПАРАЛЛЕЛЬНОГО ПОТОКОВОГО ШИФРОВАНИЯ БОЛЬШИХ ОБЪЁМОВ ДАННЫХ

*Белорусский государственный университет информатики и радиоэлектроники
г. Минск, Республика Беларусь*

Куцейко Р.Ю.

Ярмолик В.Н. – д.т.н., профессор

В настоящее время существует множество отраслей деятельности человека, которые сталкиваются с необходимостью хранения и обработки огромного количества цифровой информации на различных носителях. В случае необходимости защиты такого большого объёма данных с помощью криптографии, наибольшей проблемой становится время, необходимое на процесс шифрования и дешифрования. В связи с тем, что скорость процессорной обработки информации на сегодняшний день растёт медленно, для решения поставленной задачи необходимо использовать параллельные вычисления, обеспечивающие многократное ускорение обработки и алгоритмы, поддающиеся разбиению на параллельные процессы. В качестве такого алгоритма можно рассматривать алгоритм потокового шифрования DESX. Процесс его работы поддается разбиению на отдельные параллельные потоки, а относительно простая реализация позволяет производить преобразования на высокой скорости.

DESX – блочный потоковый алгоритм шифрования, разработанный на базе стандарта DES (DataEncryptionStandard). Основное отличие от других модификаций заключается в добавлении процедуры отбеливания ключа шифрования для увеличения криптографической стойкости [1]. В основе алгоритма шифрования лежит преобразование сетью Фейстеля, которое представлено на рисунке 1.

На схеме наглядно изображен один из последовательных раундов преобразования входного блока данных. Блок разбивается на старшую и младшую части, после чего они обрабатываются отдельно. Вычисляется образующая функция F и происходит суммирование по модулю два для определения частей блока, который будут участвовать в следующем раунде шифрования. В зависимости от избранной стратегии шифрования (электронная кодровочная книга, сцепление блоков шифрованного текста, обратная связь по шифрованному тексту и обратная связь по выходу) можно добиться различных результатов шифрования со своими уникальными особенностями [2].