Два алгоритма из рассмотренных являются оконными, потому для них необходимо определить оптимальную ширину окна. Все исследования проводились для чисел различных размерностей, которые ограничиваются размерами эллиптических групп, рекомендованных NIST кривых P-192, P-224, P-256, P-384, P-521 (число обозначает размер поля в битах). Из полученных результатов можно сделать вывод о том, что оптимальной шириной окна для алгоритма 3 является значение 5. Оптимальное значение ширины скользящего окна (алгоритм 4) приблизительно равняется 4.

После нахождения оптимальных значений для оконных алгоритмов перейдем к сравнительному анализу производительности возведения в степень по модулю всеми рассмотренными алгоритмами для чисел различной величины. График такой зависимости можно найти на рисунке 1.

Помимо описанных алгоритмов на график также включено возведение в степень по модулю стандартным методом платформы .NET. Полученные результаты позволяют сделать вывод о том, что бинарные методы обладают худшей производительностью, а оконные – лучшей. Самым лучшим методом возведения числа в степень по модулю является алгоритм с использованием скользящего окна ширины 4. Именно он и будет использован в разрабатываемой криптосистеме. Стоит заметить, что данный алгоритм на больших эллиптических группах превосходит по производительности соответствующий метод из платформы .NET, что является хорошим результатом.

Список использованных источников:

1. Menezes, A. Handbook of applied cryptography / A. Menezes, P. Van Oorschot, S. Vanstone – CRC Press, 1997.
2. St Denis, T. BigNum math: implementing cryptographic multiple precision arithmetic / T. St Denis, G. Rose, S. Vanstone – Syngress Publishing, Inc, 2006.

ВНЕДРЕНИЕ МОБИЛЬНЫХ ТЕХНОЛОГИЙ В ПРОЦЕСС ОБУЧЕНИЯ

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

Кротов Е.М.

Данилова Г.В. – м.т.н., ассистент

Отсутствие какой-либо практики использования мобильных телефонов в процессе обучения является упущением. Один мобильный гаджет может с легкость стать заменой сразу нескольким нужным предметам. Акцентирование внимания на внедрение мобильных технологий для оптимизации ведения учебы может повлиять в лучшую сторону на успеваемость учащихся.

В настоящее время абсолютное большинство людей пользуется мобильными телефонами. Гаджет стал неотъемлемой частью нашей жизни и используется ежедневно. Этот простой, функциональный и эффективный атрибут позволяет человеку оставаться на связи, где бы он ни был, не ограничиваясь лишь сотовой связью. Различные мессенджеры, социальные сети стали тем самым фактором, без которого сегодня трудно представить общение молодёжи.

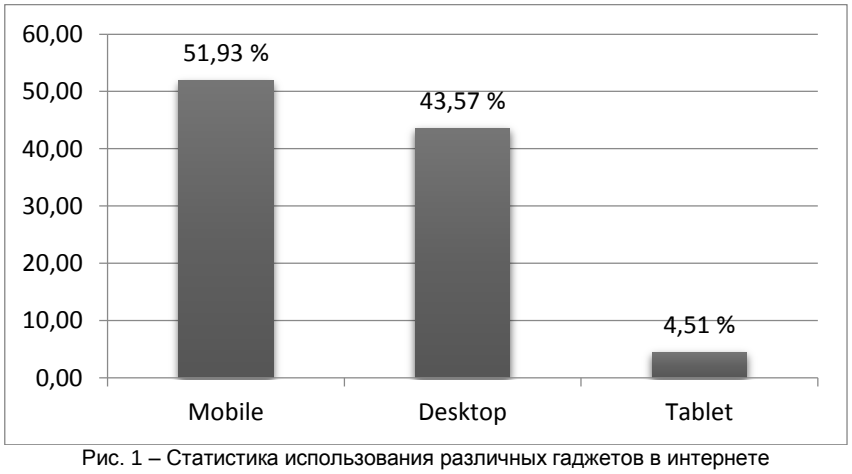

Рис. 1 – Статистика использования различных гаджетов в интернете

В то же время, преподаватели до сих пор вынуждены использовать бумагу для проведения тестов и контрольных работ. В случае, если у преподавателя много студентов, он вынужден таскать кучу макулатуры, что не только повышает риск утери чьих-то работ, но и нагружает излишним физическим трудом. Осуществлять проверку больших объемов тестов достаточно сложно и долго, при этом преподаватель сильно устает и может сам допустить ошибку, что в последствии опечалит студента и вызовет споры.

Беря во внимание данные факторы, встаёт вопрос об интеграции учебного процесса с мобильными гаджетами. Вместо огромных кип листочков с проверочными тестами, студенты могут без особых усилий

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 зарегистрированных 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 обучение, 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 актуализирование 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 чёткой 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 объёмов 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 наработать необходимую экспертизу, продуктизировать 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.