РАЗРАБОТКА И ПРИМЕНЕНИЕ ПРИКЛАДНЫХ ПРОГРАММ УЧЕБНОГО НАЗНАЧЕНИЯ ДЛЯ ОРГАНИЗАЦИИ САМОСТОЯТЕЛЬНОЙ РАБОТЫ БУДУЩИХ БАКАЛАВРОВ

Рычкова А.А.
ФГБОУ ВПО «Оренбургский государственный университет», г. Оренбург

Переход на уровневую систему подготовки кадров в соответствии с федеральными государственными образовательными стандартами аккумулирует разработку и применение в учебном процессе различных инновационных методов и средств организации самостоятельной работы студентов, в том числе дистанционных образовательных технологий на базе ИКТ.

В статье рассматривается опыт разработки и применения прикладных программ учебного назначения в ходе организации самостоятельной работы будущих бакалавров по защите информации.

В соответствии с ФГОС ВПО по направлению подготовки 090900.62 – «Информационная безопасность» одной из профессиональных компетенций, формируемых в процессе обучения, является «способность принимать участие в организации контрольных проверок работоспособности и эффективности применяемых программно-аппаратных, криптографических и технических средств защиты информации (ПК-27)», формирование которой происходит, в том числе, при изучении дисциплины базовой части профессионального цикла «Криптографические методы защиты информации». В процессе изучения данной дисциплины студенты должны знать «криптографические алгоритмы, криптографические стандарты и их использование в информационных системах» [1]. Криптография является прикладной наукой о математических методах обеспечения конфиденциальности и аутентичности (целостности и подлинности) информации, которая использует самые последние достижения математики и существенно зависит от уровня развития техники и технологии, от применяемых средств связи и способов передачи информации [2, 3, 4]. Для эффективного освоения студентами дисциплины «Криптографические методы защиты информации» в ООП ВПО предусмотрено изучение дисциплины вариативной части естественнонаучного цикла «Математические основы криптологии», в процессе освоения которой студенты будут знать основные понятия прикладной алгебры и теории чисел, уметь решать соответствующие задачи, владеть методами прикладной алгебры, навыками разработки собственных программных средств. Что служит основой понимания современных криптографических методов и средств защиты информации, таких как разработка и использование блочных симметричных криптосистем (AES), асимметричных криптосистем (RSA, El Gamal), принципа работы поточных криптосистем (на основе регистров сдвига с линейной обратной связью) и основ криптоанализа.

В таблице 1 приведены некоторые виды самостоятельной работы, формы контроля и полученные результаты будущих бакалавров по защите

информации на примере изучения дисциплины вариативной части естественнонаучного цикла «Математические основы криптологии».

Таблица 1 – Организация самостоятельной работа будущих бакалавров

Виды самостоятельной работы	Результат самостоятельной работы	Формы контроля
текущая подготовка к практическим занятиям	выполнение традиционных домашних заданий по индивидуальным вариантам	проверка домашних заданий, проведение контрольных работ
текущая подготовка к выполнению лабораторных работ	разработка собственных программных продуктов по реализации алгоритмов теории чисел, применяемых в криптографии	защита лабораторных работ
выполнение индивидуальных заданий	самостоятельное изучение теоретического материала и разработка собственных программных продуктов по индивидуальным дополнительным заданиям	проведение программно-технологической и эргономической экспертиз преподавателем с возможностью дальнейшей рекомендации к регистрации в университетском фонде электронных ресурсов лучших студенческих работ
подготовка к семинару в форме конференции	самостоятельное изучение теоретического материала по теме семинара «Традиционные системы шифрования», подготовка мультимедийной презентации.	выступление с докладом на практическом занятии, обсуждение докладов.

Основным требованием к авторскому программному средству было наличие подробного справочного руководства пользователю и программисту, подробный тестовый пример для изучения метода, понятный интерфейс. В результате выполнения студентами индивидуальных заданий было разработано 5 программных средств (участвовало 30% студентов), два из них были

представлены к регистрации в университетском фонде электронных ресурсов и в дальнейшем могут быть применены в учебном процессе.

1. Прикладная программа «Исследование чисел на простоту» ориентирована на исследование основных принципов работы с простыми числами. Основными направлениями работы являются нахождение массива простых чисел и проведение подробного анализа числа с целью выяснения его математической природы происхождения (число «простое» или «составное»). В основе программы лежат алгоритмы поиска (решето Эратосфена, решето Сундарама, решето Аткина) и тестирования числовых значений на простоту (тесты простоты Миллера-Рабина, Соловея-Штрассена, Эратосфена, Люка)

В программе предусмотрено наличие:

– теоретического материала по используемым алгоритмам поиска простых чисел и тестирования заданного числа на простоту;

– интернет ссылок по данным алгоритмам;

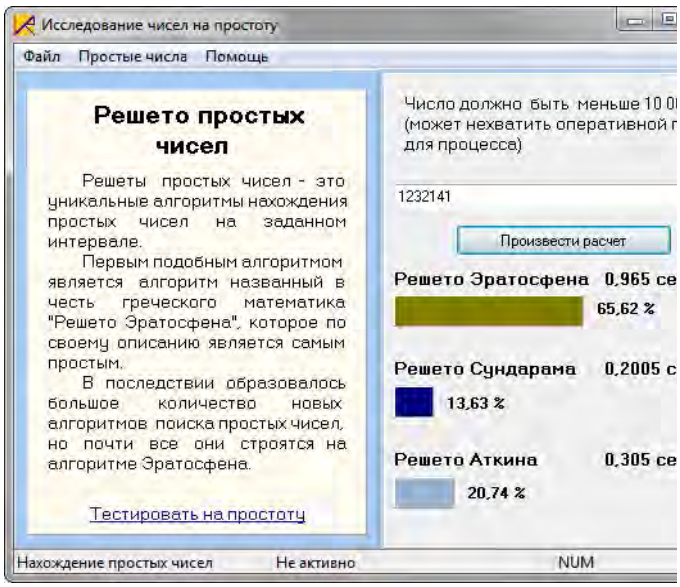
– функционального набора алгоритмов поиска простых чисел и тестирования чисел на простоту с возможностью последующего просмотра и сохранения полученных результатов в файлах формата txt.

Для теоретического ознакомления с рассматриваемыми методами нахождения простых чисел, а также тестирования чисел на простоту можно перейти в раздел теоретического материала.

В результате работы программа возвращает расчеты сразу по трем разным алгоритмам (решето Эратосфена, решето Сундарама, решето Аткина), после чего становится доступным информация о времени расчета каждого отдельно взятого алгоритма и его доли от общего времени расчета в процентах.

Пример окна программы после удачного завершения расчета простых чисел показан на рисунке 1.

Программа также производит расчет по четырем разным алгоритмам (тесты простоты Миллера-Рабина, Соловей-Штрассена, Эратосфена, Люка), после чего выводит результат о времени расчета каждого отдельно взятого алгоритма, а также процент времени каждого алгоритма от общего затраченного времени.

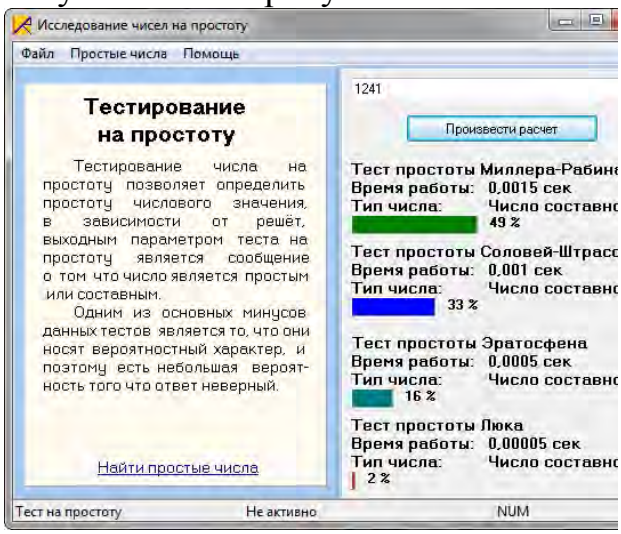


(а)

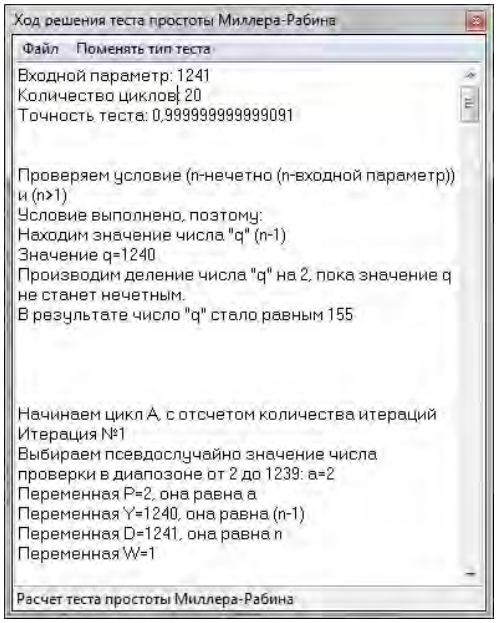
(б)

Рисунок 1 – Нахождение простых чисел на интервале (решето):
(а) – окно удачного завершения определения простых чисел на интервале;
(б) – вывод простых чисел на заданном интервале

Пример окна программы после удачного завершения теста числа на простоту показан на рисунке 2.



(а)



(б)

Рисунок 2 – Тестирование чисел на простоту:
(а) – окно удачного завершения по тестированию чисел на простоту;
(б) – вывод хода решения тестирования введенного числа на простоту.

Разработанная прикладная программа обладает следующими возможностями:

– удобный и понятный графический интерфейс программы;

– наличие понятного теоретического материала по рассматриваемым алгоритмам нахождения простых чисел и тестирования чисел на простоту;

– быстрый процесс нахождения простых чисел и тестирования чисел на простоту;

– описание полного хода решения тестирования чисел на простоту;

– наличие функционального набора алгоритмов работы с простыми числами.

2. Прикладная программа «Традиционные симметричные криптографические системы шифрования» предназначена для шифрования текстовой информации и последующего её дешифрования основными традиционными симметричными криптографическими алгоритмами замены и аналитическими преобразованиями.

Исходными данными для работы прикладной программы являются: шифруемый текст, криптографический ключ (целое положительное число или текстовое сообщение в зависимости от выбранного метода шифрования). Зашифрованная текстовая информация может быть сохранена в формате txt для последующей работы или передачи.

В прикладной программе реализованы традиционные алгоритмы симметричного шифрования методами замен и аналитическими преобразованиями текстовой информации, в которых в процессе шифрования и дешифрования информации используется один и тот же ключевой элемент (криптографический ключ).

Главное окно программы показано на рисунке 3.

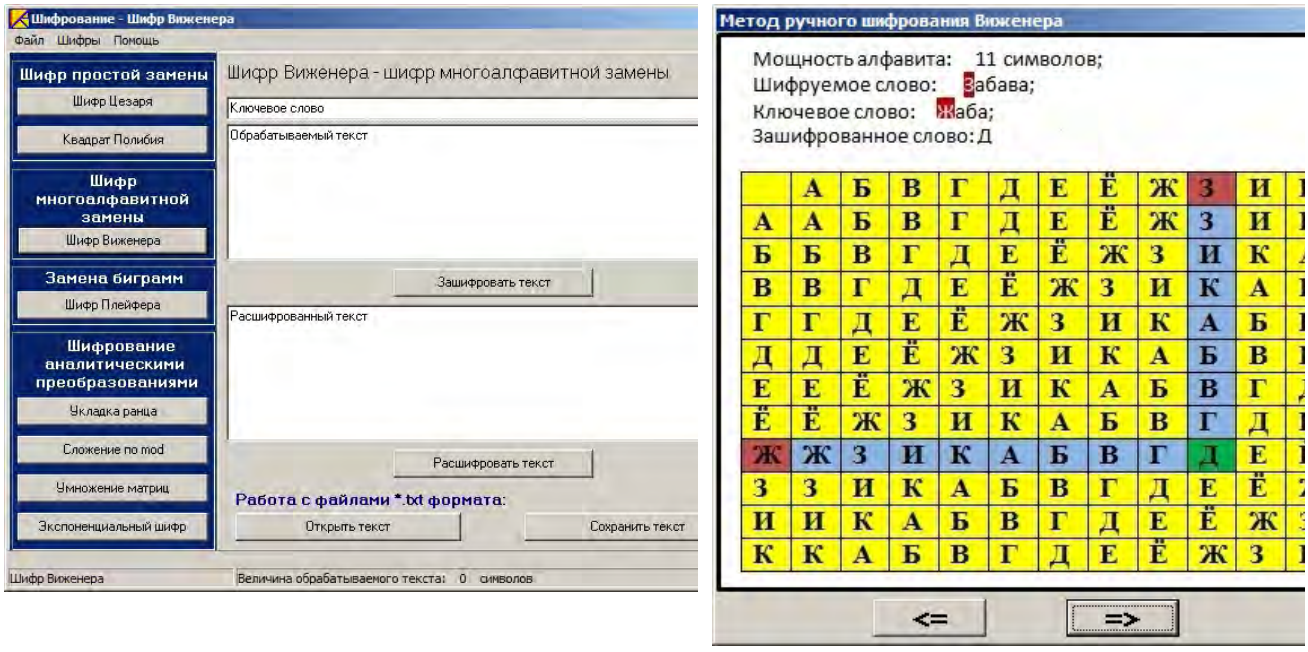


Рисунок 3 - Окна программы «Традиционные симметричные криптографические системы шифрования»

Для использования в учебном процессе в программе предусмотрено наличие:

– теоретического материала по используемым алгоритмам, которые в понятной форме поясняют процесс шифрования и дешифрования информации соответствующим алгоритмом;

– интернет ссылок по данным алгоритмам;

– функционального набора алгоритмов шифрования и дешифрования текстовой информации, с возможностью последующего сохранения полученного результата в файлах формата txt для последующей передачи и обработки данной информации;

– возможность выбора в качестве шифруемого текста готовой информации, которая находится в файлах формата txt.

Традиционные виды и формы организации самостоятельной работы в сочетании с современными средствами дистанционных образовательных технологий на базе ИКТ, такими как, прикладные программы учебного назначения способствуют активизации самостоятельной деятельности будущих бакалавров. Одним из основных педагогических условий эффективной организации самостоятельной работы будущих бакалавров является повышение личностной мотивации к выполнению индивидуальных заданий на основе работы в сотрудничестве преподавателя и студента по разработке авторского программного средства с возможностью последующей его регистрацией в университетском фонде электронных ресурсов.

Список литературы

1. Об утверждении и введении в действие федерального государственного образовательного стандарта высшего профессионального образования по направлению подготовки 090900 Информационная безопасность (квалификация (степень) «бакалавр»): Приказ от 28 октября 2009 г. № 496 (Изменения 31.05.2011 N 1975) // "Бюллетене нормативных актов федеральных органов исполнительной власти". – 2011. – 18 июля.

*2. **Нестеров, С.А.** Информационная безопасность и защита информации : учеб. пособие : пер. с англ. / С.А. Нестеров. — СПб. :Изд-во Политехн. ун-та, 2009. — 126 с. — ISBN 978-5-7422-2286-6.*

*2. **Ветров, Ю.В.** Криптографические методы защиты информации в телекоммуникационных системам: учеб. Пособие / Ю.В. Ветров, С.Б. Макаров. – СПб.: Изд-во Политехн. ун-та, 2010. – 174 с. — ISBN978-5-7422-3025-0.*

*3. **Рычкова, А.А.** Основы криптографии : мультимедийное учебное пособие / Т.Н. Шалкина, В.В. Запорожко, А.А. Рычкова. – М.: ОФАП. – 2008. – № 10602.*