Таким образом, из перечисленных условий, можно судить о том, что игровые технологии многогранны, имеют свою специфику и влияние на педагогическую деятельность учителя. Всё это будет также характерно и для компьютерных обучающих игр, как частного случая игровых технологий.

Список литературы

1. Video games bigger than film [Электронный ресурс]. – Режим доступа: http://www.telegraph.co.uk/technology/video-games/6852383/Video-games-bigger-than-film.html (дата обращения: 28.12.2016).

2. Grand Theft Auto V: It is a time to games a form of cinema? [Электронный ресурс]. – Режим доступа: http://moviepilot.com/articles/1117712-grand-theft-auto-v-is-it-time-to-consider-games-a-form-of-cinema (дата обращения: 28.12.2016).

3. Игра GTA V принесла издателям 800 млн долларов за сутки продаж [Электронный ресурс]. – Режим доступа: http://ria.ru/science/20130919/964170049.html (дата обращения: 28.12.2016).

УДК 378.016:004.056.55

И. А. Садчиков, И. А. Суслова

ИЗУЧЕНИЕ ШИФРОВАЛЬНЫХ МАШИН В РАМКАХ ИНФОРМАЦИОННЫХ ДИСЦИПЛИН

Садчиков Илья Александрович
ilyasadchikov@gmail.com
Суслова Ирина Александровна
ipik@yandex.ru
ФГАОУ ВО «Российский университет образовательных информационных технологий», Россия, г. Екатеринбург

CIPHER MACHINES STUDY IN INFORMATION SCIENCES

Sadchikov Ilya Alexandrovich
Suslova Irina Alexandrovna
ipik@yandex.ru

Russian State Vocational Pedagogical University

Аннотация. *На примере одной рассмотренной технологии студенты могут изучить полный цикл задач, связанных с передачей, защитой и взломом зашифрованных данных. В основу этой технологии положено создание и функционирование обучающего эмулятора шифровальной машины «Энигма».*

Abstract*. With help of one technology students can study full cycle of tasks associated with transfer, protection and hacking of encrypted data. Training technology was founded on emulator of Enigma encryption machine*

Ключевые слова: *шифровальная машина, Энигма, ротор, рефлектор, обучение, взлом зашифрованных данных*

Keywords: *encryption machine, Enigma, rotor, reflector, education, encrypted data hack*

Изучение шифровальных машин – одна из важнейших тем в курсах «Теоретические основы информатики», «Криптография» и «Безопасность информационных систем». В рамках темы изучаются следующие вопросы:

- история создания и практическое применение шифровальных машин различных типов;
- создание и конструктивные особенности шифровальных машин;
- принципы и алгоритмы шифрования;
- взлом шифров с помощью математического базиса и аппаратных решений;
- системы автоматизированного взлома шифров.

Очень часто в рамках курса все обозначенные выше темы изучаются в рамках лекций, тогда как практическое изучение темы связано с отсутствием имитаторов шифровальных машин, способных работать в обучающем режиме (то есть, программа может осуществить задачу шифровки / дешифровки, но не может показать студенты, как данный процесс был осуществлен на принципиальном уровне).

Для решения данной проблемы в РГППУ, было решено создать обучающий эмулятор шифровальной машины студентами третьего курса кафедры информационных систем и технологий: С. Ковехом и Т. Мартыновым (под общим руководством старшего преподавателя И. Садчикова).

Перед студентами была поставлена задача, сделать программный вариант шифровальной машины «Энигма». Компьютерная версия должна была состоять из следующих частей: клавиатуры ввода, коммутационной панели, системы роторов, рефлектора, визуального аналога телетайпа, лампочек вывода. Кроме того, в постановке задачи было указано, что компьютерная версия «Энигмы» должна была поддерживать несколько основных моделей шифровальной машины, в состав которой входили различные виды роторов и периферийных устройств. В качестве основного языка программирования был выбран C#, поскольку студенты изучали его во время учебного курса. Форматы обмена данными были реализованы на XML и jSON.

В основу системы легла базовая оболочка программы, в состав которой входил набор мета-файлов, описывающий конструктивные особенности различных видов шифровальной машины. После того, как пользователь выбирал машину, оболочка подгружала необходимые части и подпрограммы шифровального комплекса. Все без исключения варианты программной «Энигмы» имели клавиатуру, систему лампочек вывода, три ротора и рефлектор. Остальные элементы системы считались дополнительными и программа подгружала их по мере необходимости.

Программа должна была работать в двух основных режимах:

- историческом – данные вводились с шифровальную машину и сразу направлялись в виртуальные телетайп. Пользователь не мог посмотреть историю ввода данных. Исторический режим предназначался для демонстрации различных режимов работы системы во время лекций и демонстрационных показов.
- расширенном – данные вводились с шифровальную машину, визуализировались на рабочем экране и после этого направлялись в виртуальные телетайп. Пользователь мог посмотреть историю ввода данных и мог выгрузить данные во внешний файл. В расширенном режиме программа могла принимать внешние данные для расшифровки. Данный режим работы предназначался для самостоятельной работы студентов и для выполнения заданий в рамках контрольных и лабораторных работ.

Принципиальная схема реализации программы представлена на рисунке.

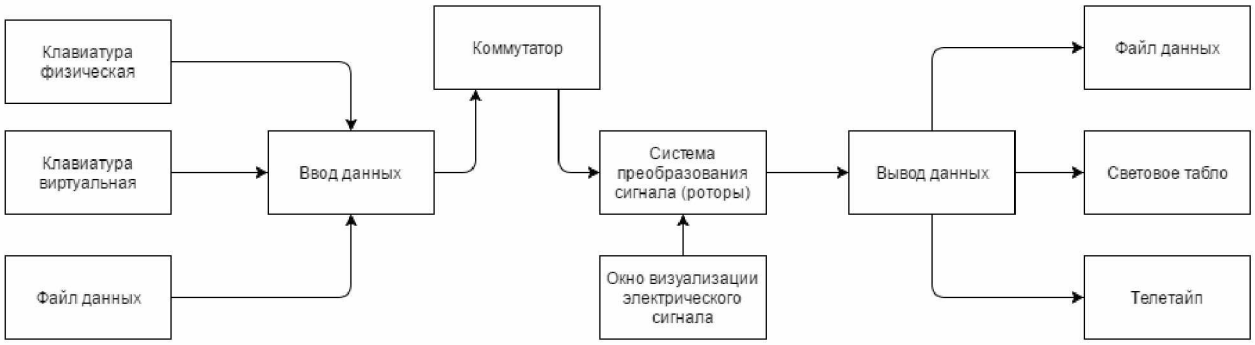

Рисунок 1 – Принципиальная схема работы программы

Ввод данных в систему осуществлялся тремя основными способами:

- виртуальная клавиатура – в этом случае пользователь набирал нужные символы в рабочем окне программы при помощи мыши;
- физическая клавиатура – в этом случае пользователь вводил данные при помощи стандартной клавиатуры, подключенной к компьютеру. Виртуальная клавиатура реагировала на нажатия и подсвечивала последний введенный пользователем символ;
- файл данных. Пользователь мог ввести данные в «Энигму» посредством XML или jSon файла. Поскольку внутри файла обмена содержались мета-данные программа могла определить на каком варианте «Энигмы» должно было произойти шифрование данных. Данная модель ввода была доступна лишь в расширенном режиме программы. В отличие от ручного ввода, файл данных мог содержать большие блоки текста, разбитые на предложения и абзацы.

Коммутационная панель шифровальной машины выводилась только на тех вариагтах «Энигмы», где она действительно была установлена. Коммутация символов осуществлялась при помощи мышки и цветовой подсветки. Таким образом, символы, находящиеся на разных концах одного коммутационного провода имели одинаковую окраску. Коммутация осуществлялась последовательно. После замыкания цепи, коммутационная подсветка меняла цвет. Нажатие на уже подсечённый символ вызывало размыкание коммутационной цепи. При необходимости пользователь мог отключить коммутационную панель и в этом случае данные сразу передавались в систему роторов.

Предварительная настройка системы роторов была реализована посредством стрелок, расположенных под окошками ввода символов. Пользователи программы могли увидеть работу роторов и рефлекторов при помощи специального окна, где визуально демонстрировалось прохождение электрического сигнала через последовательность ротора и рефлекторов. В случае ввода данных, программа визуализировала последовательность прохождения сигнала в режиме реального времени. Обратное прохождение сигнала отличалось от прямого прохождения сигнала видом подсветки. Система прохождения сигнала корректно демонстрировала конструкционные различия известных ей шифровальных машин, при этом переключение вида конструкции могло быть произведено в режиме реального времени, что вело к реконфигурации виртуальной машины.

Вывод сигнала осуществлялся одним из следующих способов:

- в историческом режиме, на визуальную панель вывода, где загоралась лампочка, соответствующая определенному символу латинского алфавита;

- в историческом режиме, на телетайп, где выходящему символу соответствовал один из элементов азбуки Морзе;
- в расширенном режиме вывод данных мог быть произведен в XML или jSON файл с последующей выгрузкой на жесткий диск или переносной носитель. Во время сохранения данных вывода, программа вносила в файл метаинформацию о текущей конфигурации системы.

После завершения внутреннего тестирования симулятор «Энигмы» прошел практическую апробацию в рамках дисциплины «Теоретические основы информатики». Программа была использована в качестве системы решения практических задач для двух групп третьего курса.

На практических занятиях были опробованы и решены следующие задачи:

- настройка шифровальных машин в соответствии с требованиями шифровальной книги;
- шифровка / дешифровка данных при помощи эмулятора и шифровальных книг;
- практические изучение принципов работы различных типов шифровальных машин;
- использование технологий защиты информации при передаче данных (ложные символы, ложные данные передачи);
- типовой взлом Энигмы при помощи виртуального аналога «Бомбы».

Таким образом, на примере одной технологии студенты изучали полный цикл задач, связанный с передачей, защитой и взломом зашифрованных данных. Тем самым на практике был реализован принцип непрерывности учебного процесса.

В дальнейшем данный эмулятор будет использован для практического обучения студентов старших курсов кафедры информационных систем и технологий, изучающих дисциплины «Теоретические основные информатики» и «Безопасность информационных систем».

УДК 371.315-028.22:[371.31:004.771]

А. В. Солодов, Е. В. Чубаркова

ВИЗУАЛИЗАЦИЯ В ДИСТАНЦИОННОМ ОБУЧЕНИИ

Солодов Андрей Валерьевич
dushe_s@mail.ru
Чубаркова Елена Витальевна
chubarkova.elena@rsvpu.ru
ФГАОУ ВО «Российский государственный профессионально-педагогический университет»
Россия, г. Екатеринбург

VISUALIZATION IN DISTANCE LEARNING

Solodov Andrew Valerevich
Chubarkova Elena Vitalevna
Russian state vocational pedagogical university Russia, Yekaterinburg

Аннотация. *В статье приводятся практические рекомендации по улучшению восприятия дистанционного курса посредством оптимизации его визуального представления.*

Abstract. *The article gives practical recommendations to improve the perception of distance course through the optimization of its visual presentation.*