УДК 378.515

АВТОМАТИЗИРОВАННЫЙ УЧЕБНО-МЕТОДИЧЕСКИЙ КОМПЛЕКС ПО ЗАЩИТЕ ИНФОРМАЦИИ И ОСНОВАМ КОМПЬЮТЕРНОЙ БЕЗОПАСНОСТИ

© В.В. Хлебников, В.А. Аверков

Ключевые слова: учебно-методический комплекс, криптография, защита информации.

В статье описан методический комплекс по курсу «Защита информации и основы компьютерной безопасности», позволяющий усовершенствовать процесс обучения, а также дающий возможность осуществлять автоматизированный централизованный сбор информации о процессе обучения для ее последующего анализа и принятия управляющих решений.

Внедрение современных способов обучения, управления информацией и программными продуктами на данный момент времени является одним из приоритетных направлений развития науки. Быстрый прогресс компьютерных технологий позволил использовать компьютерную технику в качестве эффективного средства обучения, при этом многообразие технологических решений значительно расширилось с появлением возможности широкого доступа в глобальную сеть Интернет.

В настоящее время необходимость внедрения в учебный процесс новых телекоммуникационных электронных методов и систем обучения уже не вызывает сомнений, а обучающие комплексы становятся неотъемлемой частью подготовки высококвалифицированных специалистов [1, 2].

В связи с развитием компьютерной техники, компьютерных программ и информационных технологий в последние несколько десятков лет стало возможным применение компьютера в процессе обучения. До недавнего времени компьютеры, в основном, использовались как вспомогательные средства. Основным же источником научных знаний для обучающихся являлись лекционные и семинарские занятия, проводимые преподавателями в соответствии со штатным учебным расписанием. Закрепление изученного материала, а также контроль хода учебного процесса осуществлялись посредством выполнения практических задач – лабораторных, контрольных, тестовых, экспериментальных работ и т. д.

При таком способе обучения усвоение полученных знаний осуществлялось неравномерно, что зачастую было связано с различными уровнями интеллектуального развития обучающихся [3] и скоростью усвоения нового учебного материала.

В связи с этим, ввиду индивидуальных особенностей студентов и тонкостей учебного процесса стали появляться информационные системы по различным учебным дисциплинам, выполненные в качестве компьютерных программ. Данные информационные системы позволяли проводить обучение каждого студента индивидуально, что значительно повышало уровень знаний последнего.

Контроль знаний, приобретенных при индивидуальном обучении, осуществлялся посредством тестирования. При таком подходе преподаватель может контролировать уровень успеваемости и сам процесс обучения.

В рамках существующих на данный момент времени автоматизированных обучающих систем решается ряд важных задач обучения [4]. В первую группу можно отнести задачи проверки уровня знаний, умений и навыков обучающихся до и после обучения, их индивидуальных способностей, склонностей и мотиваций. Для таких проверок обычно используют соответствующие системы тестов и экзаменационных вопросов. К этой же группе относятся задачи проверки показателей работоспособности обучающихся, осуществляющейся путем регистрации таких психофизиологических показателей [5], как скорость реакции, уровень внимания и т. д. В частности, к этой группе можно отнести всевозможные IQ-тесты, которые позволяют выявить существующий уровень интеллекта обучаемого.

Вторая группа задач связана с регистрацией и статистическим анализом показателей усвоения учебного материала: ведение индивидуальных разделов для каждого обучающегося, определение времени решения задач, определение общего числа ошибок и т. д. К этой же группе относится решение задач управления учебной деятельностью. Например, решение задач по изменению темпа предъявления учебного материала или порядка предъявления обучающемуся новых блоков учебной информации в зависимости от времени решения, типа и числа ошибок. Таким образом, эта группа задач направлена на поддержку и реализацию основных элементов программированного обучения.

Третья группа задач автоматизированных учебно-методических систем связана с проблемой подготовки и представления учебного материала, его адаптации по уровням сложности, подготовки динамических иллюстраций, контрольных заданий, лабораторных и самостоятельных работ учащихся.

Таким образом, цель данной работы заключалась в разработке автоматизированного учебно-методического комплекса по курсу «Защита информации и основы компьютерной безопасности», позволяющего

интенсифицировать процесс обучения за счет активного взаимодействия системы «студент – компьютер – преподаватель», реализующий принципы оптимального управления, а также дающий возможность осуществлять автоматизированный централизованный сбор информации о процессе обучения для ее последующего анализа и принятия управляющих решений.

Для реализации учебника по данному курсу был использован язык HTML, а в качестве редактора web-страниц использовался Macromedia Dreamweaver 8, т. к. в настоящее время наиболее распространенной технологией хранения информации на компьютере является язык HTML. Основным его достоинством является поддержка гиперссылок, позволяющих быстро перемещаться внутри документа и между ними. В такие документы можно легко вставлять различную мультимедиа информацию. Помимо перечисленных достоинств в случае разработки учебных и справочных систем исходная информация для них может быть получена из сети Интернет в том же формате, что значительно сокращает время создания системы. А для реализации учебно-методического комплекса было принято решение использовать Turbo Delphi 2006 [6–9].

Реализованный программный комплекс включает в себя следующие разделы: электронный учебник, тестируемая программа и конструктор тестов.

Созданный электронный учебник написан на языке HTML и представлен в виде классического учебника, который позволяет удобно и быстро получить необходимую информацию, просмотреть примеры реализации некоторых алгоритмов, а также пройти тест, используя гиперссылки. Внешний вид одной из глав электронного учебника представлен на рис. 1.

Содержание учебника отражает основные темы курса «Защита информации и основы компьютерной безопасности» [10–16].

После ознакомления с учебником предполагается проверка знаний путем прохождения теста. Для облегчения разработки индивидуального задания был создан «Конструктор тестов», внешний вид которого изображен на рис. 2.

С помощью данного конструктора можно быстро создать необходимый тест с любым количеством вопросов и ответов. Также возможно задать время, отводимое для прохождения, и время ответа на каждый вопрос (при желании).

Интерфейс интуитивно понятен и прост. В меню «Файл» присутствуют стандартные элементы для создания нового теста, открытия существующего, его сохранения и закрытия.

Программная структура конструктора основывается на динамическом трехмерном массиве, в котором хранится вся вводимая информация. При сохранении эта информация переписывается в файл собственного формата (*.tst). Данный формат может быть распознан либо самим конструктором (для редактирования), либо тестовой оболочкой.

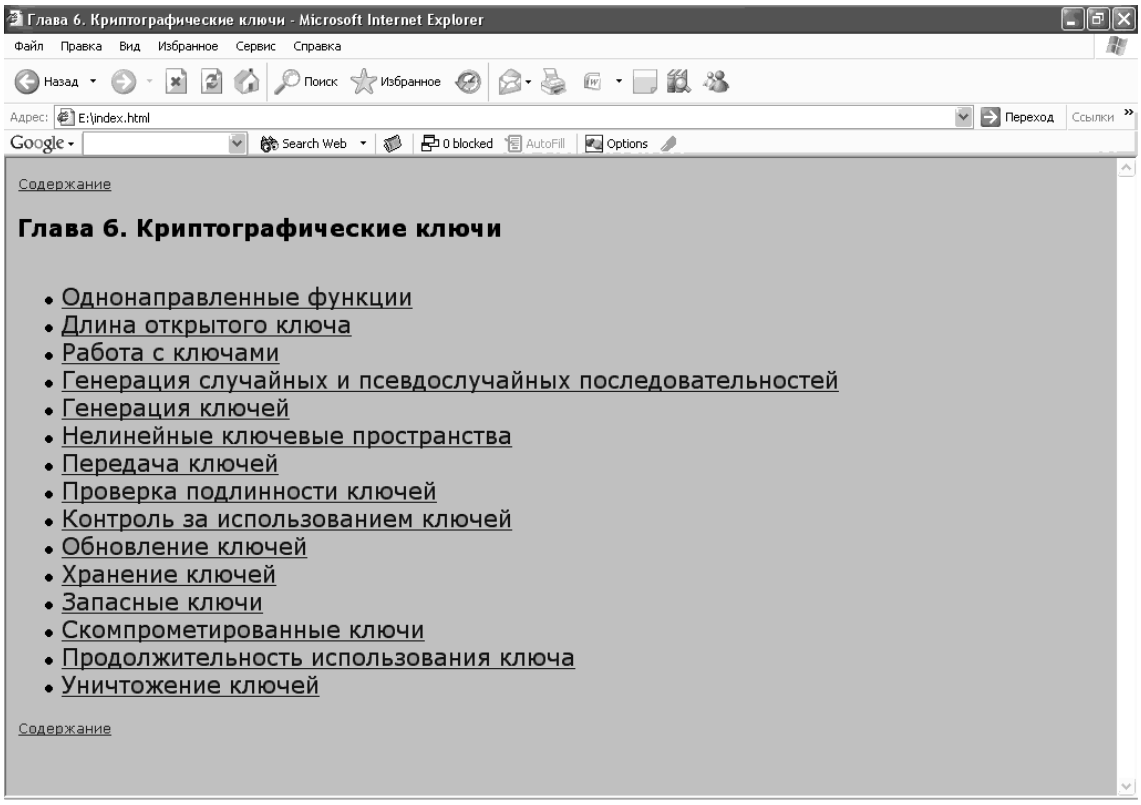

Рис. 1. Окно электронного учебника

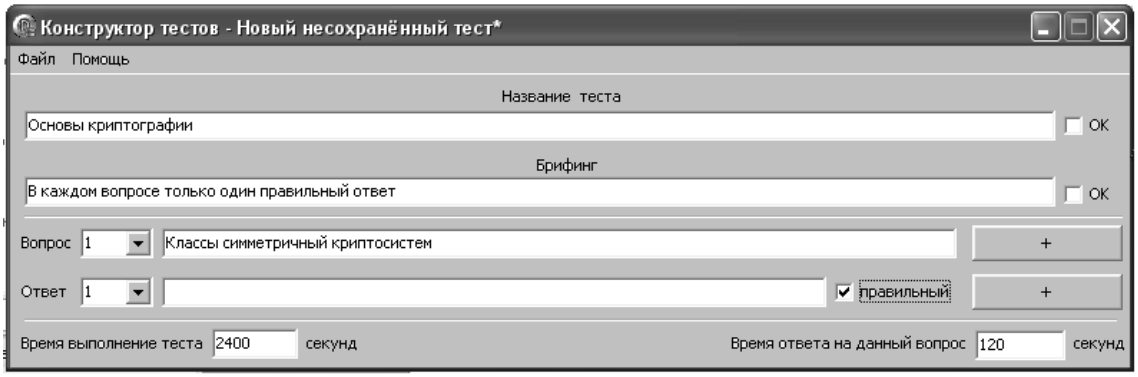

Рис. 2. Конструктор тестов

Рис. 3. Строка вопроса конструктора тестов

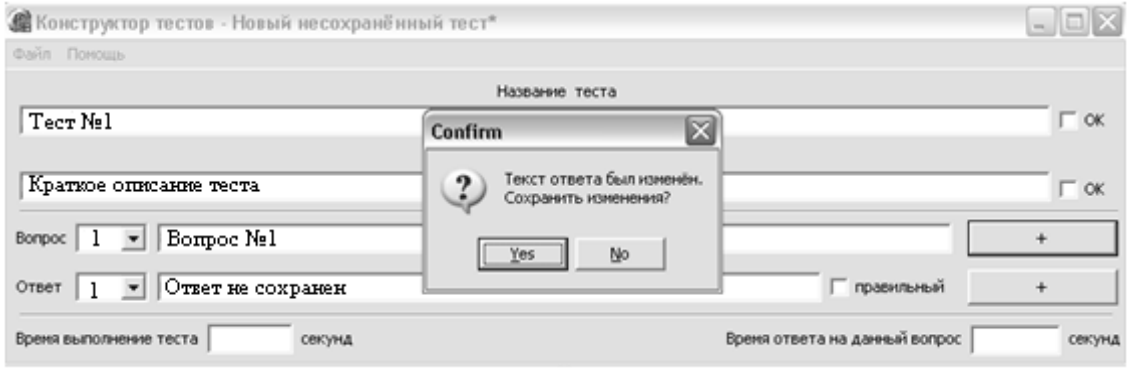

Рис. 4. Запрос на сохранение ответа

При открытии готового теста информация из файла переносится в этот массив и легко поддается любой корректировке.

Строка вопроса содержит номер текущего вопроса, его текст, кнопку сохранения и добавления следующего. В поле номера вопроса можно выбрать любой из предыдущих, уже сохраненных ранее. При этом все поля, такие как текст вопроса, текст ответа, правильность ответа, количество ответов, время, отведенное на вопрос, заполняются из массива данных. Таким образом мы можем просмотреть тексты всех ответов выбранного вопроса. Новый вопрос сохраняется в базе только после нажатия кнопки «+» (рис. 3).

Если при сохранении вопроса поле ответа не заполнено, или заполнено, но не сохранено, то будет выдано соответствующее предупреждение с запросом на сохранение ответа (рис. 4).

Строка ответа аналогична строке вопроса. Номер текущего ответа может быть изменен на любой, соответствующий количеству ответов для данного вопроса. Текст ответа при этом будет автоматически меняться.

При добавлении правильного ответа необходимо указать на это, путем установки флага «правильный». Кнопка «+» сохраняет текущий ответ в массив данных.

В нижней строке можно указать время выполнения всего теста и конкретного вопроса. Все эти данные записываются в массив и будут учтены позже. Следует учитывать, что во время ответа на вопрос входит и время на его прочтение.

При сохранении теста происходит запись данных из массива в текстовый файл собственного формата (*.tst). С этим же форматом работает сам тест, представленный на рис. 5.

После открытия теста выводится его название и краткое описание. Введенные персональные данные, как и ответы на вопросы, сохраняются во временный массив данных.

Если при выполнении теста заканчивается время, отведенное на данный вопрос, то программа информирует об этом пользователя и переходит на следующий вопрос. При окончании времени тестирования происходит автоматическое сохранение всех данных и выход из программы.

Для более удобного сбора результатов тестирования данную программу полезно располагать на компьютере преподавателя и запускать с компьютеров-клиентов учеников через сеть. Это позволит сохранять все результаты в отдельную папку, заданную преподавателем.

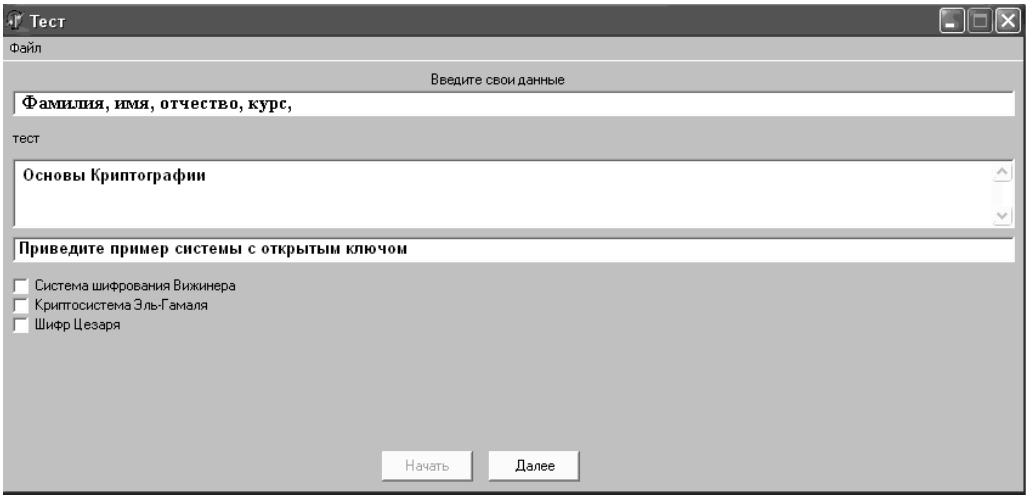

Рис. 5. Внешний вид теста

Каждый тест именуется личными данными, вводимыми учеником в начале тестирования. При этом эта информация отображается в программе-оболочке, что позволяет визуально контролировать соответствие указанных данных тому, кто проходит тест.

После завершения теста производится сравнивание введенных ответов с правильными. В итоге производится вывод информации в файл, который именуется данными тестируемого. Данный файл содержит следующую информацию: фамилию, имя, отчество, курс, группа, количество правильных ответов, общее количество вопросов, процент правильности ответов, а также список всех правильных и неправильных ответов. Это позволяет адекватнее оценить уровень знаний преподавателем, чтобы определить, в каких темах ученик отстает, и какой уровень он уже освоил.

В данной версии тестирующей программы введены следующие ограничения: максимальное количество ответов на один вопрос – 8, количество правильных ответов – 1. Ограничения в количестве вопросов нет.

Таким образом, в данной работе были рассмотрены разные виды автоматизированных обучающих систем. Каждый вид систем имел свои особенности, ввиду которых область их применения была различна. Целью данной работы являлась разработка такой обучающей системы, которая будет иметь возможность минимизировать время обучения и, в то же время, будет являться достаточно гибкой в работе.

В ходе выполнения работы были получены следующие результаты: разработана общая структура автоматизированного обучающего комплекса; реализован программно-обучающий курс по «Защите информации и основам компьютерной безопасности»; разработан конструктор тестов для последующей проверки знаний и тестовая оболочка.

ЛИТЕРАТУРА

1. *Кларин М.В.* Инновации в обучении. М.: Наука, 1997. С. 224.
2. *Мельников А.В.* Принципы построения обучающих систем и их классификация // Педагогические и информационные технологии в образовании. 2001. №4. С. 67-73.
3. *Растригин Л.А.* Адаптивное обучение с моделью обучаемого. Рига: Зинанте, 1988.
4. *Мельников А.В.* Принципы построения обучающих систем и их классификация // Педагогические и информационные технологии в образовании. 2001. №4.
5. *Суходольский Т.В.* Введение в математико-психологическую теорию деятельности. СПб.: Изд-во С.-Пб. ун-та, 1998. С. 220.
6. *Архангельский А.Я.* Программирование в Delphi 7. М.: ООО «Бином-Пресс», 2003.
7. *Бобровский С.И.* Delphi7. Учебный курс. СПб.: Питер, 2005.
8. *Гофман В.Э.* Delphi 6. СПб.: БХВ-Петербург, 2001.
9. *Фленов М. Е.* Библия Delphi. СПб.: БХВ-Петербург, 2004.
10. *Болотов А.А.* Элементарное введение в эллиптическую криптографию: Алгебраические и алгоритмические основы. М.: КомКнига, 2006.
11. *Болотов А.А.* Элементарное введение в эллиптическую криптографию: Протоколы криптографии на эллиптических кривых. М.: КомКнига, 2006.
12. *Харин Ю.С.* Математические основы криптологии: учеб. пособие. Мн.: БГУ, 1999.
13. *Кузнецов Г.В.* Математические основы криптографии: учеб. пособие. Днепропетровск: Национ. ун-т, 2004.
14. *Нечаев В.И.* Основы теории защиты информации. М.: Высш. шк., 1999.
15. *Птицын Н.* Приложение теории детерминированного хаоса в криптографии. М.: МГТУ им. Баумана, 2002.
16. *Макконнелл С.* Совершенный код. Мастер-класс / пер. с англ. М.: Издат.-торговый дом «Русская редакция»; СПб.: Питер, 2005.

Поступила в редакцию 27 сентября 2008 г.

Khlebnikov V.V., Averkov V.A. Automated educational methodical course of basics of computer and information security. This article describes the methodical complex for the course “The Basics of computer and information security” that allows improving the learning process and gives us an ability to automate an information gathering process for the further analysis and managerial decision making.

Key words: educational-methodical complex, encoding, information security.

LITERATURE

1. *Klarin M.V.* Innovation in training. M.: Nauka, 1997. P. 224.
2. *Melnikov A.V.* Principles of training systems development and their classification // Pedagogical and Information Technologies in Education. 2001. #4. P. 67-73.
3. *Rastrigin L.A.* Adaptive training with a model of a trainee. Riga: Zinante, 1988.
4. *Melnikov A.V.* Principles of training systems development and their classification // Pedagogical and Information Technologies in Education. 2001. #4.
5. *Sukhodolsky T.V.* Introduction to the mathematical-psychological theory of activity. SPb.: St. Petersburg University Publishing House, 1998. P. 220.

6. *Arkhangelsky A.Y.* Programming in Delphi 7. M.: LLC "Bin-Press", 2003.
7. *Bobrovsky S.I.* Delphi7. The Training course. SPb.: Piter, 2005.
8. *Gofman V.E.* Delphi 6. SPb.: BKV-Peterburg, 2001.
9. *Flenov M.E.* Delphi Bible. SPb. M.: BKV-Peterburg, 2004.
10. *Bolotov A.A.* Elementary introduction to elliptic cryptography: Algebraic and algorithmic bases. M.: Komkniga, 2006.
11. *Bolotov A.A.* Elementary introduction to elliptic cryptography: Reports of cryptography on elliptic curves. M.: Komkniga, 2006.
12. *Kharin Y.S.* Mathematical basis of cryptology: textbook. Minsk: BSU, 1999.
13. *Kuznetsov G.V.* Mathematical basis of cryptography: textbook. Dnepropetrovsk: National University, 2004.
14. *Nechaev V.I.* Bases of the information protection theory. M.: Vysshaya Shkola, 1999.
15. *Ptitsyn N.* Application of the theory of the determined chaos in cryptography. M.: MSTU named after Bauman, 2002.
16. *McConnell P.* The perfect code. The master-class / translation from English. M.: Trading House «Russian Edition»; SPb.: Piter, 2005.