УДК 37.01

ОПТИМИЗАЦИЯ ОБУЧЕНИЯ ПО ТЕМЕ «ОСНОВЫ КРИПТОГРАФИИ» ОБУЧАЮЩИХСЯ ЮРИДИЧЕСКИХ СПЕЦИАЛЬНОСТЕЙ

Еськин Д. Л., Бакулин В. М.

ФГКОУ ВО «Волгоградская академия МВД России», Волгоград, Россия, email: yd38@bk.ru

В статье предложена методика проведения практического занятия по теме «Основы криптографии» в гуманитарном вузе. Рассмотрены основные проблемы, которые возникают при реализации традиционной методики: отсутствие наглядности, наличие большого количества ошибок вследствие обработки объемной символьной информации, плохое ориентирование обучающихся внутри русского алфавита. Для решения указанных проблем была разработана специальная обучающая программа, которая облегчает процесс освоения простейших криптографических преобразований и способствует активизации познавательной деятельности обучающихся. В статье описаны интерфейс, алгоритм действий и особенности данной обучающей программы, а также подробно описаны действия обучаемых в процессе ее использования во время практического занятия. В конце статьи приводятся результаты апробации применения данной программы в процессе обучения студентов юридических специальностей по дисциплине «Основы информационной безопасности».

Ключевые слова: методика обучения, криптография, информационная безопасность, программное обеспечение.

OPTIMIZATION OF TRAINING ON "BASICS OF CRYPTOGRAPHY" STUDENTS OF LEGAL SPECIALTIES

Eskin D. L., Bakulin V. M.

Volgograd Academy of the Ministry of the Interior of the Russian Federation, Volgograd, Russia, e-mail: yd38@bk.ru

The paper proposes a method of practical training on "Basics of cryptography" in a liberal arts college. The main problems that arise in the implementation of the traditional method: the lack of clarity, the large number of errors due to processing volume symbol information, poor orientation of students in the Russian alphabet. To solve these problems, we developed a special training program, which facilitates the development of simple cryptographic transformations and helps enhance the cognitive activity of students. The article describes the interface algorithm of actions and characteristics of the training program, as well as the detailed action of students in the course of its use during the practice session. At the end of the article presents the results of testing of this program in teaching law students on the subject "Fundamentals of Information Security".

Keywords: training technique, cryptography, information security, software.

В современном обществе профессиональная деятельность человека находится в тесной взаимосвязи с различными информационными технологиями, так как именно они позволяют сделать работу специалиста комфортной, быстрой и максимально эффективной. Однако нужно понимать, что одних современных технологий для повышения эффективности труда недостаточно. Необходимо, чтобы специалист умел ими пользоваться, а также мог соблюдать нормы по обеспечению защиты информации [1].

Одним из эффективных методов защиты информации является криптографическое преобразование информации или криптография. Подробное изучение криптографии требует от специалиста определенного уровня владения математическим аппаратом. В силу того, что непосредственно с информацией часто приходится работать людям нетехнических специальностей (например, юристам), для них важно понять сам принцип использования

криптографического преобразования и то, от каких его параметров будет зависеть сохранность информации [2].

Проще всего добиться этой цели, изучая простейшие алгоритмы криптографического преобразования, которые не требуют от обучающегося специфических математических знаний. Предлагаемая в данной работе методика изучения основ криптографического преобразования основана на проведении практических занятий, в ходе которых обучающимся будет проще понять основные принципы шифрования, а также оценить важность такого параметра, как ключ шифрования. Целями обсуждаемого занятия являются:

- формирование у обучающихся понимания сущности криптографического преобразования информации, а также назначения ключа как важнейшего элемента алгоритма шифрования;
- освоение навыков использования различных методов криптографического преобразования, а также навыков криптоанализа зашифрованной информации различными методами.

Традиционный вариант проведения практического занятия по данной теме предусматривает применение в процессе письменного решения обучающимися в тетрадях задач применения различных алгоритмов шифрования информации с последующими письменными упражнениями в зашифровке, расшифровке и криптографическом анализе текстовых данных без использования средств вычислительной техники.

В процессе такого обучения возникают проблемы, связанные с: а) отсутствием наглядности процесса шифрования; б) наличием большого количества ошибок вследствие выполнения обучающимися ручной обработки объемной символьной информации; в) плохой ориентировкой обучающихся внутри русского алфавита, в частности, с трудностями в определении символов, предшествующих данной букве или следующих за ней, что особенно ярко проявляется при обучении слушателей иностранных государств. В результате при выполнении заданий обучающиеся не могут сконцентрировать свое внимание на центральном моменте зашифровывания/расшифровывания – ключе алгоритма шифрования.

Замысел разработки и создания специальной компьютерной программы для занятия состоял в наглядном представлении различных алгоритмов шифрования информации с использованием инструментов, облегчающих процесс зашифровки и расшифровки сообщений для исключения основных объемов рутинной работы обучающихся. Помимо этого программа в автоматическом режиме должна была облегчить проверку полученных в течение занятия навыков с использованием заранее подготовленной базы текстовых сообщений. Кроме того, использование интерактивных обучающих программ во время

практических занятий способствует активизации познавательной деятельности обучающихся [3, 4].

С учетом всего этого авторами данной работы была создана специализированная программа для ЭВМ [5], предназначенная для использования при проведении практического занятия с обучающимися. Рассмотрим более подробно ее особенности.

В начале работы с программой обучающемуся предлагается пройти регистрацию, после чего идентификационные данные курсанта указываются в заголовочной части главного окна программы. Далее курсанту предлагается изучить теоретическую часть, посвященную основам шифрования и криптоанализа, либо сразу перейти к выполнению практических заданий.

В случае выбора изучения теоретического курса в главной рабочей области программы постранично представляется теоретический материал. Следует отметить, что у обучающегося всегда присутствует возможность в случае необходимости вернуться к изучению теоретической части на любом этапе работы с программой.

После ознакомления с теоретическими основами шифрования и криптоанализа обучающиеся переходят к непосредственному выполнению практических заданий, которое проходит в три последовательных этапа.

На первом этапе работы обучающиеся практикуются в зашифровке сообщений методом простого сдвига. В качестве ключа шифра здесь выступает величина сдвига. При этом на экран выводятся (рисунок 1):

– исходный текст, который необходимо зашифровать обучающемуся;

– окно, указывающее величину сдвига, на который обучающийся должен зашифровать текст;

– окно для ввода зашифрованного текста;

– окно, указывающее число правильных ответов, полученных при выполнении заданий из данного блока;

– окно, указывающее число ошибок, допущенных при выполнении заданий из данного блока;

– окно с отображением двух алфавитов – обычного и со сдвигом, предназначенное для удобства обучающегося и позволяющее уменьшить время на рутинную работу по переписыванию алфавита вручную на бумаге.

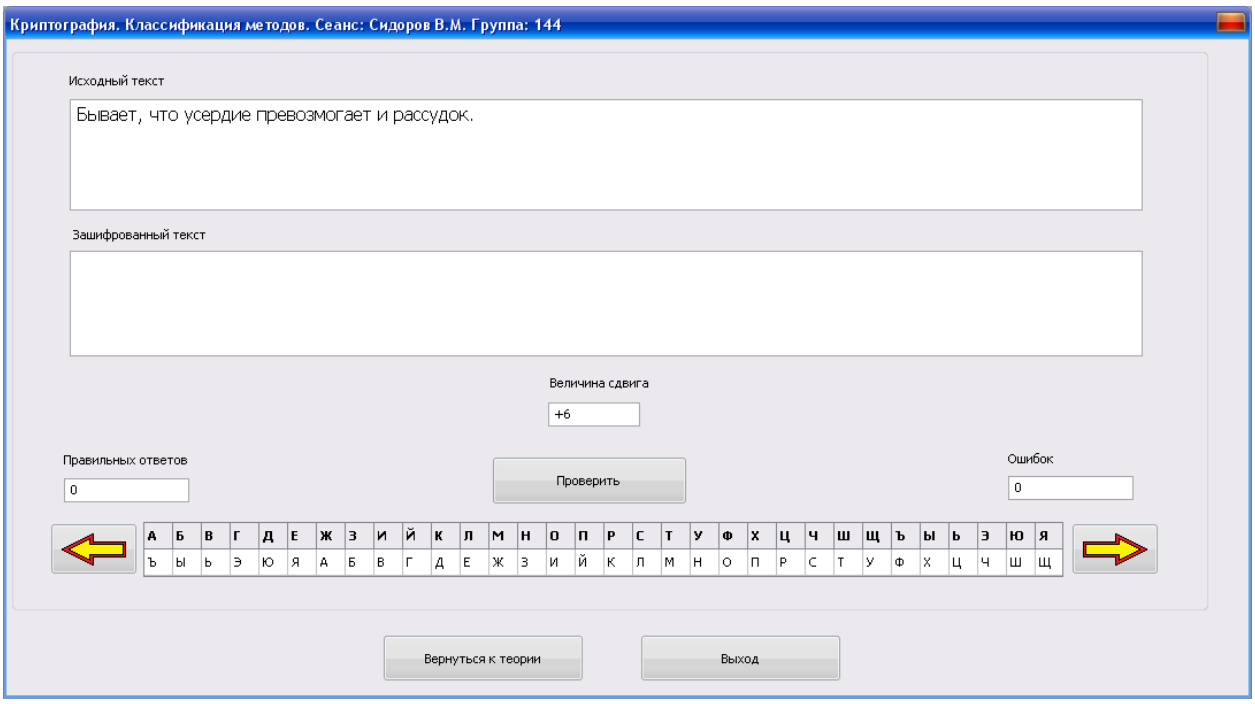

Рис.1. Практическое задание первого блока

Выбор исходных текстов для зашифровывания не случаен. В качестве заданий обучающимся предлагаются пословицы и поговорки назидательного характера, несущие не только функциональную, но и воспитательную нагрузку. Всего в базе исходных текстов содержится порядка 700 пословиц, поговорок и крылатых фраз, из которых в качестве задания случайным образом выбирается одна.

Формирование ключа шифрования, т.е. величины сдвига, происходит также с помощью датчика случайных чисел. Данный подход сводит к нулю вероятность совпадения заданий различных обучающихся. После нажатия на кнопку «Проверить» происходит автоматическая проверка введенного текста на правильность, о чем сообщается в соответствующем всплывающем окне. Если обучающийся дал правильный ответ, то происходит генерация следующего задания из данного блока.

Число заданий в блоках задается преподавателем в служебных настройках программы. После выполнения всех заданий из блока число совершенных обучающимся ошибок отображается в заголовочной части окна программы.

Следующий этап практического занятия посвящен криптографическому анализу сообщений, зашифрованных простейшим методом – методом простого сдвига. Для этого созданная нами программа предлагает обучающимся расшифровать текстовую информацию без знания ключа шифра. Как и на предыдущем этапе, исходная фраза случайным образом выбирается из базы исходных текстов, а далее происходит ее автоматическая зашифровка на величину сдвига, полученную с помощью датчика случайных чисел. Для того чтобы

уменьшить количество ручной работы, на экран выводится простой алфавит и алфавит со сдвигом, величина которого определяется пользователем программы.

На третьем этапе курсанты осваивают метод перестановок с использованием матриц на практике. Задание осложняется тем, что при зашифровке сообщений из текста удаляются все пробелы и знаки препинания, в результате чего полученный в процессе расшифровки текст необходимо дополнительно анализировать и разбивать по словам, исходя из смысловой нагрузки полученной фразы. Исходный текст для криптоанализа получается путем шифрования методом перестановок с помощью квадратной матрицы, размер которой выбирается случайным образом в пределах от 3x3 до 7x7, фразы, выбираемой случайным образом из базы фраз. Для повышения эффективности и наглядности освоения метода на экран выводится матрица перестановок с соответствующим образом заполненными ячейками. Размер матрицы выполняет роль ключа шифрования и задается пользователем.

После выполнения всех заданий открывается итоговое окно работы с программой, содержащее идентификационные данные пользователя, а также число ошибок, которые были им допущены в каждом из блоков заданий.

Предложенная методика проведения практического занятия с использованием специально созданного программного обеспечения была апробирована на практических занятиях по дисциплине «Основы информационной безопасности» у обучающихся юридических специальностей. По результатам проведенных занятий можно сказать, что эффективность изучения основ криптографического преобразования информации существенно повысилась за счет уменьшения рутинной однотипной работы и повышения продуктивности. Кроме того, нельзя не отметить повышение познавательного интереса обучающихся к изучению данной темы при использовании указанной программы.

Список литературы

1. Бакулин В.М., Бедрин В.С. Программно-техническое обеспечение формирования информационных компетенций // Современные проблемы науки и образования. – 2015. – № 4. – С. 237.

2. Бакулин В.М. Основные вопросы информационной безопасности // Вестник Волгоградской академии МВД России. – 2010. – № 4. – С. 126-129.

3. Еськин Д.Л., Бакулин В.М. Применение интерактивных обучающих компьютерных программ в процессе вузовского обучения // Процесс формирования компетенций: проблемы эффективности: сб. науч. тр. – Волгоград: ВА МВД России, 2015. 1 электрон. опт. диск (CD-R).

4. Еськин Д.Л., Бакулин В.М. Современные обучающие компьютерные программы: основные требования //Актуальные вопросы в научной работе и образовательной деятельности сборник научных трудов по материалам Международной научно-практической конференции: в 10 т. – Тамбов, 2015. – С. 75-76.
5. Свид. о гос. Регистрации программы для ЭВМ №2015617732 от 21 июля 2015 г. РФ, МПК (нет). Программная поддержка занятия «Основы криптографии: метод сдвига» / Д.Л. Еськин, В.М. Бакулин. – 2015.

Рецензенты:

Разбегаева Л.П., д.п.н., профессор, профессор кафедры всеобщей истории и методики преподавания истории и обществоведения Волгоградского государственного социально-педагогического университета, г. Волгоград;

Ходякова Н.В., д.п.н., доцент, начальник кафедры информатики и математики Волгоградской академии МВД России, г. Волгоград.