УДК 372.862

Н.А. Горбунова, Н.Н. Синкевич
Карагандинский университет им. академика Е.А. Букетова
Караганда, Казахстан

ПРИМЕНЕНИЕ WEB-КВЕСТА ДЛЯ ПРОМЕЖУТОЧНОГО И ИТОГОВОГО КОНТРОЛЯ ПРИ ОБУЧЕНИИ ШИФРОВАНИЮ

Аннотация. *Использование информационных технологий раскрывает огромные возможности компьютера, как средства обучения и контроля. Представленный web-квест позволяет сформировать у обучающихся интерес к дисциплине, дает оптимальное усвоение рабочего материала, развивает интеллектуальную самостоятельность.*

N. A. Gorbunova, N.N. Sinkevich
Karaganda University named after Academician E.A. Buketov
Karaganda, Kazakhstan

WEB-QUEST USE FOR MIDTERM AND FINAL CONTROL DURING ENCRYPTION TEACHING

Abstract. *The use of information technology reveals the enormous potential of the computer as a means of teaching and control. The presented web-quest allows students to form an interest in the discipline, provides optimal assimilation of working material, and develops intellectual independence.*

В процессе использования web-квестов студенты учатся выстраивать свою работу по алгоритму, выявлять закономерности и представлять результаты проведенной работы. Web-квесты являются эффективной формой активизации образовательной деятельности студентов, повышают интерес к изучаемой дисциплине [1].

На главной странице web-квеста по шифрованию обучающегося встречает мотивационное сообщение: «Научитесь шифрованию! Здесь можно ознакомится и практически применить простые и популярные методы шифрования, представленные в форме web-квеста». А также, важная рекомендация: «Приготовьте ручку и бумагу и обязательно запишите тот логин, который введете при регистрации, он вам обязательно понадобится».

Предоставлена возможность перехода на страницу для ознакомления с правилами прохождения web-квеста, и на страницу регистрация/авторизация.

В приложении реализовано два уровня доступа, это авторизация преподавателя и обучающегося.

Обучающемуся предусмотрена регистрация для прохождения web-квеста с целью обучения и получения практических навыков в шифровании, а также для прохождения контрольных точек, предусмотренных в рамках изучаемой дисциплины.

Преподавателю реализована возможность просмотра отчетов о деятельности обучающегося и резервирование исходного текста для шифрования.

На странице, где можно ознакомится с правилами прохождения web-квеста по шифрованию, представлен следующий текст: «В порядке установленной очередности вам будут открываться различные методы шифрования. Переход на следующий этап осуществляется при условии правильно зашифрованного данным методом вашего логина, указанного при регистрации».

В различных методах шифрования, реализованных в данном квесте, понадобится исходная фраза для шифрования, для этого отлично подойдет указанный логин при регистрации. Реализованные алгоритмы квеста будут шифровать по правилам указанного метода введенный пользователем логин и полученный результат сравнивать с введенным ответом пользователя на странице метода. При совпадении этап квеста будет считаться пройденным.

На странице регистрации обучающегося, предлагается указать фамилию и имя в качестве логина и группу. При самостоятельном использовании квеста обучающимся возможен произвольный ввод данных. Главное, что текст, введенный в поле «Фамилия Имя» и будет являться исходным текстом для шифрования во всех методах. При прохождении контрольных точек преподаватель может создать по вариантам различные исходные фразы и их нужно будет ввести обучающемуся в поле «Фамилия Имя».

Рассмотрим в качестве примера один из этапов квеста представленный на рисунке 1. Шифр одинарной перестановки. На главной странице представлен краткий информационный материал о методе шифрования и показан практический пример шифрования данным методом фамилии «ИВАНОВ».

В общем случае для данного класса шифров при шифровании и дешифровании используется таблица перестановок. В первой строке данной таблицы указывается позиция символа в исходном сообщении, а во второй – его позиция в шифрограмме [3].

Например, возьмем следующую таблицу перестановок и зашифруем сообщение «ИВАНОВ»

1	2	3	4	5	6
2	4	1	3	6	5

Впишем исходное сообщение, переставим буквы согласно таблице и выпишем шифрограмму.

1	2	3	4	5	6
И	В	А	Н	О	В
2	4	1	3	6	5
В	Н	И	А	В	О

Шифрограммой будет «ВНИАВО».

В задании указано: «Используйте свой логин, указанный при регистрации для участия в web-квесте, зашифруйте его с помощью указанной таблицы перестановок и введите в поле ответов. При правильно введенной шифрограмме вы сможете перейти к следующему методу».

Указанная таблица перестановок формируется в случайном порядке, предварительно считывая количество символов, указанных в логине при регистрации. На данном изображении логин при регистрации был длинной 12 символов, начиная с нулевой позиции в случайном порядке формируется перестановка.

Так же предусмотрена кнопка «Пропустить», дающая возможность перейти на следующий этап квеста, в случае невозможности или нежелания прохождения данного этапа. Данное действие будет заносится в отчет о прохождении квеста с формулировкой «Метод шифрования был пропущен пользователем».

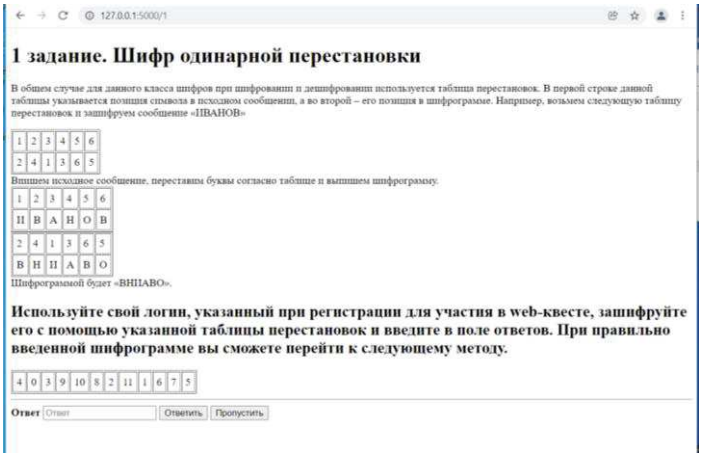

Рис. 1 – Этап web-квеста, шифр одинарной перестановки

Еще один метод – шифрование с использованием «магического квадрата». На странице web-квеста, показанной на рисунке 2,

представлено краткое описание метода и показан практический пример шифрования.

Рассмотрим квадрат размером 4х4. В него вписываются числа от 1 до 16. Его магия состоит в том, что сумма чисел по строкам, столбцам и полным диагоналям равняется одному и тому же числу – 34. Пример такого квадрата [3]:

16	3	2	13
5	10	11	8
9	6	7	12
4	15	14	1

Шифрование по магическому квадрату производится следующим образом. Например, требуется зашифровать фразу: «ИВАНОВИВАНОВИВАН». Буквы этой фразы вписываются последовательно в квадрат согласно записанным в ячейках числам.

16 Н	3 А	2 В	13 И
5 О	10 Н	11 О	8 В
9 А	6 В	7 И	12 В
4 Н	15 А	14 В	1 И

Пример шифрования с помощью магического квадрата

После этого шифрованный текст записывается в строку (считывание производится слева-направо сверху-вниз, построчно) – «НАВИОНОВАВИВНАВИ».

Для оптимального времени выполнения задания был выбран «магический квадрат» размерностью 4х4. В алгоритмах квеста формируется магический квадрат для пользователя, на сегодняшний день «магических квадратов» 4х4 насчитывается уже 880, это более чем достаточное количество для различных вариантов.

В задании указано: Используйте свой логин, указанный при регистрации для участия в web-квесте, запишите его без пробелов, добавьте символ «.», так, чтобы получилось 16 символов вместе с логином. Далее используя указанный «магический квадрат», зашифруйте строку, и введите в поле ответа. При выполнении всех действий правильно вы сможете перейти к следующему методу.

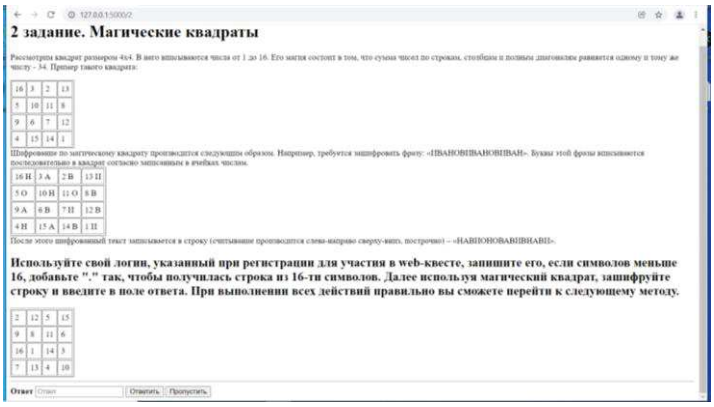

Рис. 2 - Этап web-квеста, шифр «магические квадраты»

Так же реализована возможность пропустить этап.

Завершающая страница квеста будет содержать информацию о прохождении квеста, будет указанно количество попыток, что именно вводилось в поле ответов каждого метода, случаю пропусков этапов квеста и итоговый результат.

Данная информация хранится в созданной базе данных, так же будет доступна преподавателю для ознакомления и возможности формирования соответствующих выводов о уровне знаний и умений обучающегося в области шифрования данных различными методами.

Модель обучения, основанная на интерактивных методах, меняет роль преподавателя в учебном процессе. Если ранее преподаватель являлся источником знаний и информации, то теперь он трансформируется в помощника и консультанта, организатора и координатора занятий [2]. Изменяется и содержательная часть изучаемого предмета, а также форма подачи заданий.

Представленная разработка позволяет преподавателю дать возможность обучающимся апробировать на практике и закрепить теоретические знания о методах шифрования, а также проводить промежуточный и итоговый контроль по темам, связанным с методами шифрования в различных дисциплинах, в которых предусмотрена тематика шифрования и кодирования.

Список использованных источников

1. Ваганова О.И., Гладков А.В., Булаева М.Н. Использование скрайбинга и веб-квеста в образовательном процессе // БГЖ. 2021. №2 (35).

2. Саранцев Г. И. Нужны ли интерактивные формы обучения? // Проблемы современного математического образования в вузах и школах России: Интерактивные формы обучения математике

студентов и школьников: Материалы V Всеросс. науч.-методич. конф, Киров: Изд-во ВятГГУ, 2012. – С. 42–48.

3. Учебная и научная деятельность Анисимова Владимира Викторовича - Шифры перестановки (google.com)

УДК 581.522.4:582.688.3:634.73

Д.В. Гордей, В.В. Сосновский, В.С. Зелинская
Белорусский государственный технологический университет
Минск, Республика Беларусь

ПОТЕНЦИАЛ ИНТРОДУЦИРОВАННЫХ ВИДОВ СЕМЕЙСТВА ERICACEAE В РАЗВИТИИ ПРОМЫШЛЕННОГО ЯГОДОВОДСТВА НА НАРУШЕННОЙ ЧАСТИ ТОРФЯНИКА ДОЛБЕНИШКИ

Аннотация. *Успешное развитие промышленного ягодоводства в экстремальных погодно-климатических и эдафических условиях верховых торфяников Белорусского Поозерья возможно с привлечением голубики узколистной, а также межвидовых гибридов голубики высокорослой и голубики узколистной. Хозяйственная ценность клюквы крупноплодной требует подтверждения.*

D.V. Gordey, V.V. Sosnovskiy, V.S. Zelinskaya
Belarusian State Technological University
Minsk, Republic of Belarus

THE POTENTIAL OF INTRODUCED SPECIES OF THE ERICACEAE FAMILY IN THE DEVELOPMENT OF INDUSTRIAL BERRY GROWING ON THE DISTURBED PART OF THE DOLBENISHKI PEAT BOG

Abstract. *The successful development of industrial berry growing at the extreme weather, climatic and soil conditions of the raised peatlands of the Belarusian Poozerie is possible with the involvement of lowbush blueberries, as well as interspecific hybrids of highbush blueberries and lowbush blueberries. The economic value of cranberries requires confirmation.*

В 2021 г. видовой состав ягодников живого напочвенного покрова выбывшего из эксплуатации в 80-х гг. XX ст. торфяного месторождения верхового типа Долбенишки был представлен голубикой топяной (Vaccinium uliginosum L.), брусникой обыкновенной (Vaccinium vitis idaeae L.) и клюквой мелкоплодной