

Создание активных методов обучения криптографии при помощи MS Excel

Анна Сергеевна Зуфарова

Старший преподаватель кафедры «КБ»
Тихоокеанский государственный университет
Хабаровск, Россия
006694@pnu.edu.ru
ORCID 0000-0000-0000-0000

Юлия Сергеевна Бузыкова

Доцент кафедры МОСИТ
МИРЭА-Российский технологический университет
Москва, Россия
juliaserg_buz@mail.ru
ORCID 0000-0000-0000-0000

Поступила в редакцию 20.01.2024
Принята 20.02.2024
Опубликована 15.03.2024

УДК 004.492:51:681.3

DOI 10.25726/b8190-7254-5061-f

EDN OKGVEQ

ВАК 5.8.2. Теория и методика обучения и воспитания (по областям и уровням образования)
(педагогические науки)

OECD 05.03.HE EDUCATION, SPECIAL

Аннотация

В нынешнее время существует проблемы повышения качества отечественного образования, в связи с этим необходимо совершенствовать не только информационные технологии, техническое обеспечение, но и образовательные технологии. Современные потребности в высокопрофессиональных специалиста в области информационной безопасности невозможно осуществить без перестройки системы профессиональной подготовки кадров. Из-за этого необходимо внедрить активные методы обучения в учебный процесс. Актуальность данной темы обусловлена тем, что изучение исторических шифров является неотъемлемой частью в изучении криптографических методов защиты информации. Изучение исторических шифров с использованием MS Excel позволяет проводить анализ больших объемов данных и облегчает работу с числовыми и текстовыми данными. Данный продукт предназначен для создания таблиц, различных расчетов, визуализации данных и построения графиков и многое другое, что делает его полезным инструментом для изучения основ криптографии. В изучении исторических шифров MS Excel позволяет исследователям проводить анализ частотности букв, слов и биграмм, выполнять различные математические операции для расшифровки текстов, создавать статистические модели для анализа шифров. Также с помощью этого приложения можно использовать пользовательские функции и макросы для автоматизации решений классических задач криптографии. Что способствует качественному обучению учащихся основам криптографии. Благодаря своей популярности и простоте использования MS Excel может стать популярным инструментом в исследованиях исторических шифров, анализе данных и обучении основ криптографии. Так же его применение имеет большую актуальность в современных исследованиях криптографии, например RSA, протокол Диффи-Хелмана.

Ключевые слова

активные методы обучения, имитационные методы обучения, неимитационные методы обучения, упражнения, криптография, шифр, исторические шифры, шифр Цезаря, защита информации, пользовательские функции, макросы, MS Excel.

Введение

Криптография (κρυπτός «скрытый» + γράφω «пишу») с греческого переводится тайнопись. Основной задачей криптографии является защита информации от несанкционированного доступа и утечки данных. В данный момент она используется для защиты данных в коммуникациях, банковском деле, электронной коммерции и многих других областях. Однако для успешной реализации криптографических технологий необходимо правильно обучать специалистов в этой области (Минюк, 2014).

В этом контексте педагогика может играть ключевую роль. Методы обучения защите информации должны быть основаны на классических и современных принципах педагогики.

Материалы и методы исследования

Активные методы обучения — это способы активизации учебно-познавательной деятельности студентов, которые побуждают их к активной мыслительной и практической деятельности в процессе овладения материалом, когда активен не только преподаватель, но и студенты.

Преподаватель не должен работать в направлении изложения готового материала знаний и контролировать процесс воспроизведения «из-под палки» (Зуфарова, 2020).

Основа активных методов обучения – это диалог между педагогов и студентами, а также между самими учащимися. Благодаря таким процессам в обучении развиваются коммуникативные способности, развивается речь студентов, учащиеся учатся решать проблемы коллективно, лучше усваивают материал.

Активные методы способствуют к привлечению учащихся к самостоятельной и познавательной деятельности, вызывает личностный интерес к поставленной задаче и решению ее. Так же возможность применения студентами полученных знаний, которые пригодятся в дальнейшей профессиональной деятельности (Зуфарова, 2024).

Результаты и обсуждение

Методы активного обучения применяются на различных этапах учебного процесса и можно выделить три пласта (Сдвижков, 2024).

Первый пласт – первичное овладение знаниями: проблемная лекция, учебная дискуссия, беседа, обучающие тренажеры и многое другое.

Второй пласт – закрепления знаний: мини самостоятельные, тестирование, коллективное мышление, упражнение, и другое.

Третий пласт – формирование профессиональных умений и навыков, способность развитие творческой деятельности. На этом этапе используем игровые и неигровые методы обучения: имитационное упражнения, имитационное моделирование, кейсы, деловая игра, разыгрывание ролей, инновационная игра и другое.

Рассмотрим критерии применения активных методов обучения: принципы обучения; цели и задачи обучения; соответствие содержанию темы; учебные возможности учащихся: возрастной ценз, психологический и подготовительный уровень, условие и время обучения учащихся; дополнительные средства обучения (технически оснащенные помещения, виртуальные комнаты); компетенции и возможности самих педагогов (предшествующий опыт, педагогические навыки, личностные качества педагога) (Анашкина, 2011)

Можно условно классифицировать активные методы обучения как имитационные и неимитационные (рис.1).

Имитационные методы можно разделить на игровые и неигровые. К игровым методам можно отнести: игровое проектирование, разыгрывание ролей, деловая игра, инновационная игра, организационно-десятилистная игра, мероприятие «лабиринт», квест и многое другое (Кашапов, 2001).

К неигровым методам можно отнести: кейс-технология, групповой тренинг, имитационное упражнение, анализ конкретных ситуаций.

К неимитационным методом относятся: проблемные лекции, тематические дискуссии, групповая консультация, презентация, олимпиада, упражнения, доклад, опрос-ответ, самостоятельное чтение, «жужжащие» группы, мозговой штурм и многое другое.



Рисунок 1. Классификация активных методов обучения

Благодаря имитационным методом обучения происходит воспроизведение среды профессиональной деятельности. Это способствует успешному решению проблемных ситуаций. Такие занятия предусматривают воспроизведение индивидуальной и коллективной деятельности учащихся.

Неимитационные методы обучения не требуют модели, которые применяются в имитационном обучении. Здесь стимуляция обеспечивается прямыми и обратными связями между учащимися и педагогом (Курьянов, 2011).

Свой взгляд остановим на нужных нам методах обучения. Рассмотрим понятия: упражнение, систематическое упражнение, имитационное упражнение.

Упражнение – этот метод предполагает, что учащийся сознательно и многократно повторяет умственные и практические действия с целью закрепления и совершенствования необходимых навыков и умений для дальнейшей профессиональной деятельности.

Систематическое упражнение – это метод предполагает, что учащийся будет выполнять данные задания систематически, что способствует эффективному формированию умений и навыков. Только есть один минус – это побуждающая функция.

Функция метода упражнения – заключается в преобразовании часть знаний в навыки и умения, а также сформировать практические действия, творческую активность. Диагностическое значение упражнения заключается в том, что учащиеся понимает, что приобретенные знания помогают овладеть умением и навыкам для их дальнейшего обучающего процесса.

Имитационные упражнения – это один из активных методов обучения, особенность его состоит в том, что заранее известно только преподавателю оптимальное решение проблемы, можно сказать, что

это имитационная игра. В ней не моделируется деятельность специалистов, а только остается модель среды.

С помощью этих методов можно обеспечить эффективное усвоение студентами материала по криптографии и его успешное применение в практической деятельности.

Кроме того, использование современных образовательных технологий может значительно облегчить процесс обучения в защите информации. Например, использование знания MS Excel для изучения криптографических алгоритмов позволит студентам проводить практические эксперименты и тестировать свои знания без необходимости приобретения дорогостоящего оборудования, но это на первых этапах изучения. Знание основных принципов криптографии позволяет специалистам в области информационных технологиях создавать безопасные системы передачи и хранения данных (Кыстаубаева, 2014).

В учебной программе по информационным технологиям важно вводить учащихся различных заведений в мир криптографии, чтобы они понимали, как защищать информацию, осознавали угрозы безопасности и знали методы защиты. Знание криптографии позволит будущим специалистам создавать безопасные и надежные системы, обеспечивая защиту данных и конфиденциальность информации. Понимать, как строятся алгоритмы защиты, где есть уязвимые места в системах и многое другое.

Как раз, на этих занятиях учащиеся познают все о защите данных – проходят методы шифрование, модульную математику, теория чисел и многое другое. Но на первом этапе ребята проходят исторические шифры.

К историческим шифрам относятся шифр Цезаря, шифр Виженера, квадрат Полибия, лозунговый шифр, шифр Тритемия, шифр Белазо и многие другие. Знакомятся с древними методами защиты данных. Понимают и разбирают на учебных занятиях, что за чем идет, как применять тот или иной алгоритм.

Исторические шифры играли огромную роль в обмене секретной информацией в течение многих веков, начиная с простейших замен букв, и до сложных механических и электронных устройств. Изучение исторических шифров помогает понять, для чего нужна та или иная операция в современных алгоритмах шифрования. Актуальность данной темы обусловлена тем, что изучение исторических шифров является неотъемлемой частью в изучении криптографических методов защиты информации.

MS Excel хотя и не предназначена специально для криптографии, может быть полезной в данной области благодаря своим функциям для работы с данными и математическими операциями.

MS Excel – это инструмент для работы с данными, который может быть использован при изучении основ криптографии, например при изучении исторических шифров. С его помощью можно проводить различные анализы, создавать таблицы, графики и диаграммы, которые помогут в расшифровке кодов.

Благодаря MS Excel можно составить один из активных методов обучения: упражнения. Рассмотрим его ниже и разберем различные подходы для создания упражнений.

Один из самых известных шифровых текстов – это шифр Цезаря, который был использован именно Юлием Цезарем во время войн Галлов и Британии. Шифр Цезаря является частным случаем шифра простой замены.

В этом шифре каждая буква заменяется на букву, находящуюся на определенное количество позиций в алфавите. Например, при замене на 3 позиции буква А станет D, буква В станет Е и т.д. Если мы знаем количество позиций, на которое были сдвинуты буквы шифра Цезаря, то преобразование назад можно легко выполнить с помощью таблицы в Excel вручную. Рассмотрим пример: зашифруем слово «Лекция», ключ 5. Получается «РКПЫИД» (рис. 2).

На первом этапе знакомства с историческими шифрами этот простой пример подходит для школьников и студентов в изучении и принципе понимания шифрование шифром Цезаря. Создается вуалированная таблица данных, по ней происходит анализ шифра и принцип работы. Такое упражнение можно отнести к систематическим упражнениям. Педагог может разработать такие задания на все исторические шифры и применять их в первые 5-10 мин на занятиях, для эффективного формирования навыков и умения.

1	А	Б	В	Г	Д	Е	Ж	З	И	Й	К	Л	М	Н	О	П	Р	С	Т	У	Ф	Х	Ц	Ч	Ш	Щ	Ъ	Ы	Ь	Э	Ю	Я	Задание 1.1	
2	Е	Ж	З	И	Й	К	Л	М	Н	О	П	Р	С	Т	У	Ф	Х	Ц	Ч	Ш	Щ	Ъ	Ы	Ь	Э	Ю	Я	А	Б	В	Г	Д	s=5	Лекция
3					2		5		3	1												4										6	Ркпынд	
4																																		
5	А	Б	В	Г	Д	Е	Ж	З	И	Й	К	Л	М	Н	О	П	Р	С	Т	У	Ф	Х	Ц	Ч	Ш	Щ	Ъ	Ы	Ь	Э	Ю	Я	Задание 1.2	
6	Ь	Ь	Э	Ю	Я	А	Б	В	Г	Д	Е	Ж	З	И	Й	К	Л	М	Н	О	П	Р	С	Т	У	Ф	Х	Ц	Ч	Ш	Щ	Ъ	s=-5	Реферат
7	6				2											1	7	3															Лапалын	
8					4											5																		

Рисунок 2. Шифр Цезаря

На втором этапе для создания активных методов обучения – упражнения, хорошо подходят встроенные функции MS Excel. В Excel есть множество встроенных функций, которые могут быть полезны при изучении криптографии. Рассмотрим реализацию шифра Цезаря в MS Excel по следующему алгоритму.

1. Лист_1: напечатать алфавит (A1-A40), выделить этот диапазон ячеек и присвоить выбранному алфавиту имя «ABC».

2. Лист_2: ввести текст в ячейку B1,

– C6 ввести формулу =ПОИСКПОЗ(B6;ABC;0), находит номер буквы в массиве ABC.

Копируем формулу в ячейки C7-C47.

– В D6 вводим формулу

=ЕСЛИ(ПОИСКПОЗ(B6;ABC;0)+\$D\$4>40;ПОИСКПОЗ(B6;ABC;0)+\$D\$4-40;ПОИСКПОЗ(B6;ABC;0)+\$D\$4), это сдвигаем нумерацию алфавита для кодирования текста.

– В ячейку E6 вводим формулу «=ИНДЕКС(ABC;D6)». Копируем формулу в ячейки E7-E47.

– Чтобы кодировать текст, в ячейку F6 пишем «=E6», в ячейку F7 – «=F6&E7». Копируем формулу из ячейки F7 в ячейки F8-F47.

– В ячейку B3 ввести формулу «=ПРОПИСН(B1)».

– В D3 введем формулу «=ДЛСТР(B3)»,.

– Введем число k в ячейку D4.

– В столбце A, начиная с ячейки A6, пронумеруем ячейки числами от 1 до N, N – число символов в тексте, считая пробелы.

– В B6 набрать формулу «=ПСТР(B\$3;A6;1)», чтобы разделить текст посимвольно. Далее копируем формулу в ячейки B7-B47.

3. Лист_3: на третьем листе дешифруем как в предыдущих пунктах, учитывая, что: напечатать шифртекст; в ячейку D6 ввести формулу:

=ЕСЛИ(ПОИСКПОЗ(B6;ABC;0)-\$D\$4<0;ПОИСКПОЗ(B6;ABC;0)-\$D\$4+40;ПОИСКПОЗ(B6;ABC;0)-\$D\$4).

В MS Excel есть удобная функция – копирование формул и показ формул, что облегчается учащимся в данной работе.

Разработан алгоритм для шифра Цезаря. Так же можно расширить это упражнения, добавив другие исторические алгоритмы шифрования. На этом этапе не нужно особо знать программирование. Нужно ориентироваться на алгоритмизацию и встроенные функции Excel.

Благодаря таким упражнениям педагог помогает учащимся в познание работы с основными встроенными функция MS Excel и понимании принципов работы криптографии. Это второй вид упражнений, который создан благодаря MS Excel.

Третий вид упражнений – это создание пользовательских функций в Excel.

На этом этапе студенты могут создать функцию для шифрования текста с использованием определенного алгоритма. Например, шифр Цезаря, лозунговый шифр, шифр Полибия, шифр Третемиа, шифр Белазо, шифр Виженера.

Для создания пользовательской функции в Excel используется язык программирования VBA (Visual Basic for Applications). Язык программирования VBA имеет синтаксис, схожий с другими версиями Visual Basic, и предоставляет широкий набор функций и методов для работы с приложениями Microsoft

Office. У него простой и понятный синтаксис, что делало его идеальным для новичков в программировании.

The image displays two screenshots of an MS Excel spreadsheet. The top screenshot shows a grid of numbers and letters (A-Z) with a highlighted path. The bottom screenshot shows the resulting decrypted text 'ГАЙ ЮЛИЙ ЦЕЗАРЬ ПРИШЕЛ УВИДЕЛ ПОБЕДИЛ'.

А	В	С	Д	Е	Ф	Г
1	Гай Юлий Цезарь: "Пришел, увидел, победил!"					
2						
3	гай юлий цезарь: "пришел, увидел, победил!"		42			
4			3			
5						
6	1 Г	12	13	Ж		
7	2 А	8	11 В	ЗВ		
8	3 Й	18	21 М	ЖВМ		
9	4	3	6 I	ЖВМ I		
10	5 Ю	39	2	ЖВМ I,		
11	6 Л	20	23 О	ЖВМ I, О		
12	7 И	17	20 Л	ЖВМ I, ОЛ		
13	8 Й	18	21 М	ЖВМ I, ОЛМ		
14	9	3	6 I	ЖВМ I, ОЛМ I		
15	10 Ц	31	34 Ш	ЖВМ I, ОЛМ I Ш		
16	11 Е	14	17 И	ЖВМ I, ОЛМ I Ш И		
17	12 З	16	19 К	ЖВМ I, ОЛМ I Ш И К		
18	13 А	8	11 В	ЖВМ I, ОЛМ I Ш И К В		
19	14 Р	25	28 У	ЖВМ I, ОЛМ I Ш И К В У		
20	15 Ь	36	39 Ю	ЖВМ I, ОЛМ I Ш И К В У Ю		
21	16 ;	4	7 ;	ЖВМ I, ОЛМ I Ш И К В У Ю ;		
22	17 "	5	8 А	ЖВМ I, ОЛМ I Ш И К В У Ю А		
23	18 П	24	27 Т	ЖВМ I, ОЛМ I Ш И К В У Ю А Т		
24	19 Р	25	28 У	ЖВМ I, ОЛМ I Ш И К В У Ю А Т У		
25	20 И	17	20 Л	ЖВМ I, ОЛМ I Ш И К В У Ю А Т У Л		
26	21 Ш	34	37 Ы	ЖВМ I, ОЛМ I Ш И К В У Ю А Т У Л Ы		
27	22 Е	14	17 И	ЖВМ I, ОЛМ I Ш И К В У Ю А Т У Л Ы И		
28	23 Л	20	23 О	ЖВМ I, ОЛМ I Ш И К В У Ю А Т У Л Ы И О		
29	24 ,	2	5 "	ЖВМ I, ОЛМ I Ш И К В У Ю А Т У Л Ы И О "		
30	25	3	6 I	ЖВМ I, ОЛМ I Ш И К В У Ю А Т У Л Ы И О " I		
31	26 У	28	31 Ц	ЖВМ I, ОЛМ I Ш И К В У Ю А Т У Л Ы И О " I Ц		
32	27 В	11	14 Е	ЖВМ I, ОЛМ I Ш И К В У Ю А Т У Л Ы И О " I Ц Е		
33	28 И	17	20 Л	ЖВМ I, ОЛМ I Ш И К В У Ю А Т У Л Ы И О " I Ц Е Л		
34	29 Д	13	16 З	ЖВМ I, ОЛМ I Ш И К В У Ю А Т У Л Ы И О " I Ц Е Л З		
35	30 Е	14	17 И	ЖВМ I, ОЛМ I Ш И К В У Ю А Т У Л Ы И О " I Ц Е Л И		
36	31 Л	20	23 О	ЖВМ I, ОЛМ I Ш И К В У Ю А Т У Л Ы И О " I Ц Е Л И О		
37	32 ,	2	5 "	ЖВМ I, ОЛМ I Ш И К В У Ю А Т У Л Ы И О " I Ц Е Л И О "		
38	33	3	6 I	ЖВМ I, ОЛМ I Ш И К В У Ю А Т У Л Ы И О " I Ц Е Л И О " I		
39	34 П	24	27 Т	ЖВМ I, ОЛМ I Ш И К В У Ю А Т У Л Ы И О " I Ц Е Л И О " I Т		
40	35 О	23	26 С	ЖВМ I, ОЛМ I Ш И К В У Ю А Т У Л Ы И О " I Ц Е Л И О " I Т С		

А	В	С	Д	Е	Ф
	ЖВМ I, ОЛМ I Ш И К В У Ю А Т У Л Ы И О " I Ц Е Л И О " I Т С Д И З Л О А				
			42		
			3		
1	Ж		15	12	Г
2	В		11	8	А
3	М		21	18	Й
4	I		6	3	Г
5	,		2	39	Ю
6	О		23	20	Л
7	Л		20	17	И
8	М		21	18	Й
9	I		6	3	Г
10	Ш		34	31	Ц
11	И		17	14	Е
12	К		19	16	З
13	В		11	8	А
14	У		28	25	Р
15	Ю		39	36	Ь
16	;		7	4	;
17	А		8	5	"
18	Т		27	24	П
19	У		28	25	Р
20	Л		20	17	И
21	М		37	34	Ш
22	И		17	14	Е
23	О		23	20	Л
24	"		5	2	,
25	I		6	3	Г
26	Ц		31	28	У
27	Ф		14	11	В

Рисунок 3. Реализация шифра Цезаря с помощью функций MS Excel

Учащиеся на этом этапе познакомятся с алгоритмизацией и программированием. Так же ребята, научатся создать собственные пользовательские функции в MS Excel, которые в дальнейшем обучении им пригодятся.

Шифр Виженера								
Ключ	b	a	n	k	b	a	n	k
Сдвиг	2	1	14	11	2	1	14	11
Исходный текст	r	e	g	i	s	t	e	r
Зашифрованный текст	t	f	u	t	u	u	s	c
Расшифрованный текст	r	e	g	i	s	t	e	r

Шифр Виженера						
Ключ	л	и	т	в	и	х
Сдвиг	12	9	19	3	9	22
Исходный текст	ш	е	л	е	с	т
Зашифрованный текст	д	о	ю	и	ъ	и
Расшифрованный текст	ш	е	л	е	с	т

Рисунок 4. Реализация шифра Виженера с помощью функций MS Excel

На этом этапе учащиеся создают пользовательскую функцию, рассмотрим код программы для шифра Цезаря в Excel и вызов полученной пользовательской функции (рис. 5 и рис. 6).

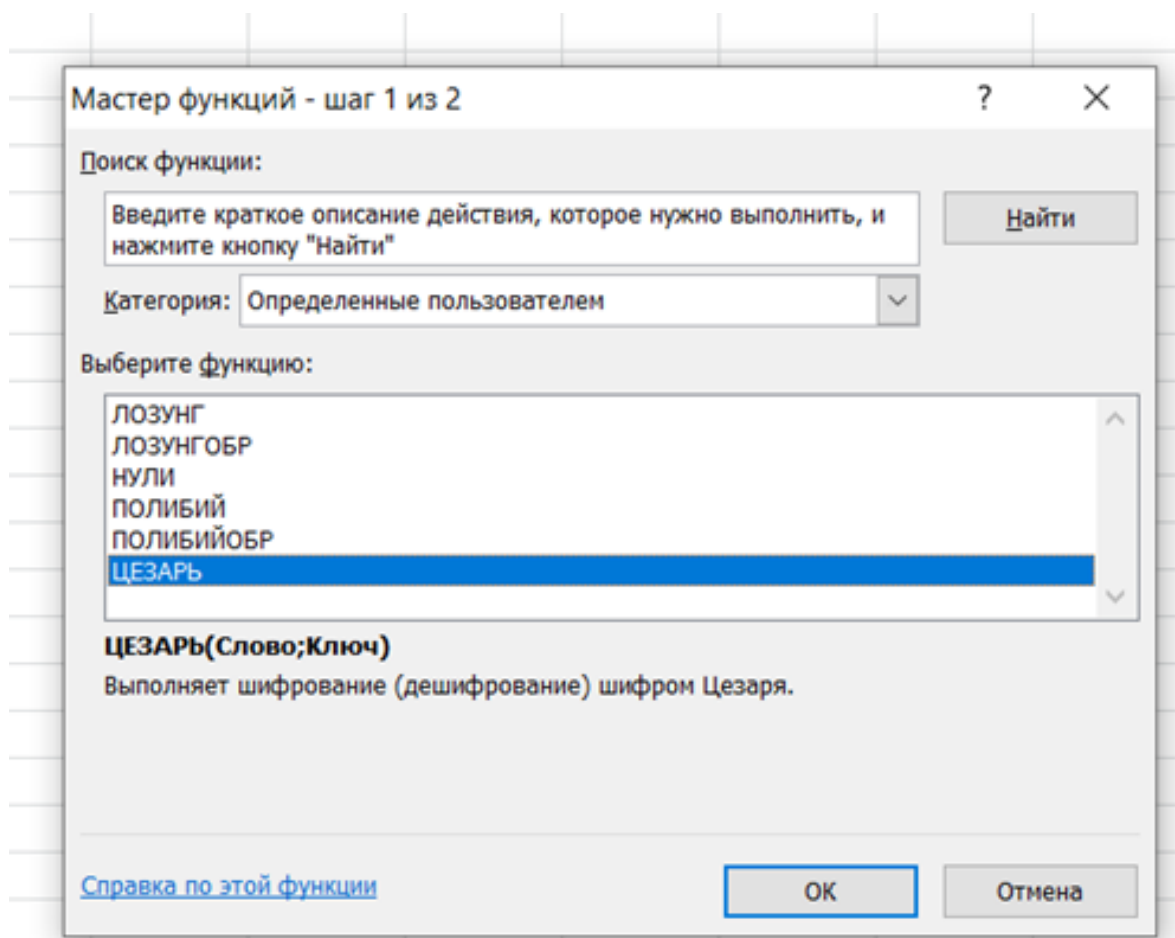


Рисунок 5. Вызов готовых пользовательских функций

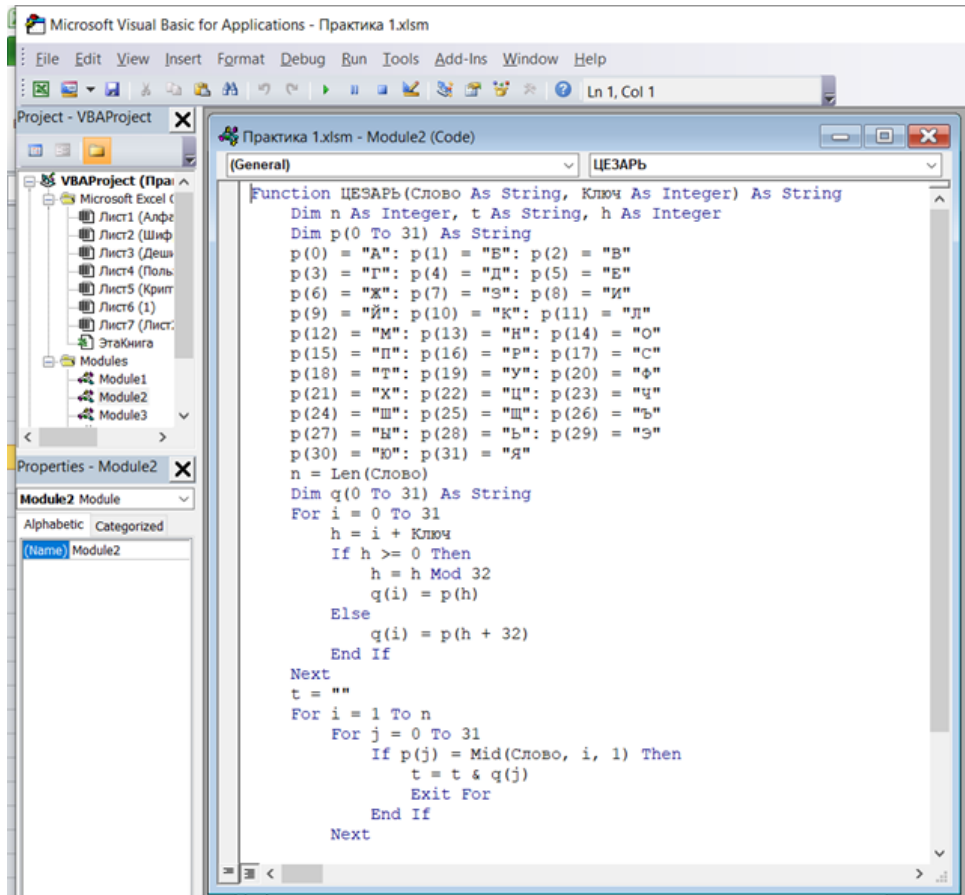


Рисунок 6. Код программы шифра Цезаря

Теперь учащиеся могут использовать функцию ЦЕЗАРЬ в ячейках Excel. Например, в ячейке А1 вы можете написать формулу `=ЦЕЗАРЬ("ЛЕКЦИЯ", 5)`, и она вернет зашифрованное значение "РКПЫНД" (Рис.7).

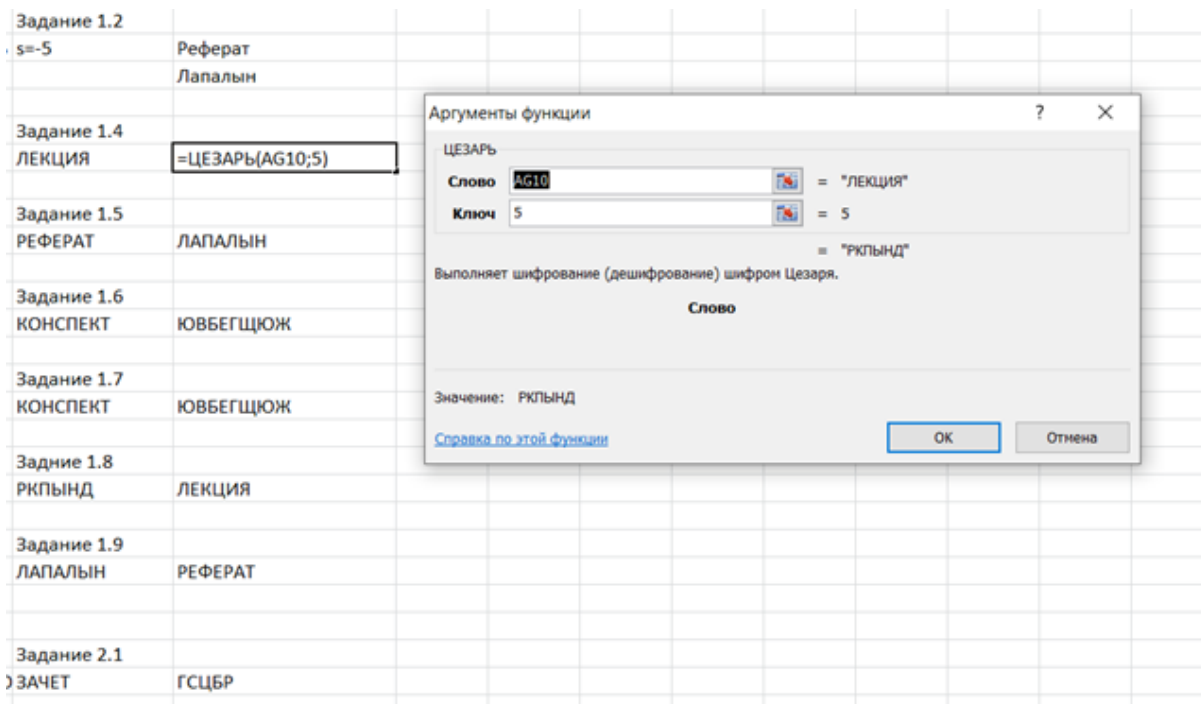


Рисунок 7. Пользовательская функция ЦЕЗАРЬ

Так педагог может осуществить и другие алгоритмы шифрования для третьего вида упражнений (рис. 8).

Макросы в Excel могут быть использованы в активных методах обучения в криптографии. С помощью его можно создать различные кейс-задания, интерактивные квесты, имитационные упражнения.

Например, можно написать макрос, который применяет различные методы шифрования, такие как шифр Цезаря или шифр Виженера, к ячейкам с данными в таблице Excel. Учащиеся должны разгадать шифр. На первом этапе учащиеся должны взломать шифр имея только ключи и шифр; на втором этапе учащиеся являются командой перехватчиков, должны взломать шифр –не имея при этом никаких ключей, на руках только шифрограмма.

Тритемий			
Ключ	Слово	Шифрование	Расшифрование
	КОНЪЮНКЦИЯ	КППЭВТРЭРИ	КОНЪЮНКЦИЯ

Белазо			
Ключ	Слово	Шифрование	Расшифрование
БАЙТ	ИНФОРМАТИКА	=БЕЛАЗО(С8;В8)	ИНФОРМАТИКА

Виженер			
Ключ	Слово	Шифрование	Расшифрование
2468	ДИЗЪЮНКЦИЯ	ЕЛМБЯРПЭЙВ	ДИЗЪЮНКЦИЯ

Аргументы функции

БЕЛАЗО

Слово: ИНФОРМАТИКА

Ключ: БАЙТ

Значение: ИНЗАСМЙДЖКЙ

Задание 2.4	ЗАЧЕТ	=Г(AG37;"СЕССИЯ")
Задание 2.5	КОЛЛОКВИУМ	ЖКЗЭЮКМГУИ
Задание 2.7	ГСЦБР	ЗАЧЕТ
Задание 2.8	ЖКЗЭЮКМГУИ	КОЛЛОКВИУМ
Задание 3.2	EXCEL	1553131531
Задание 3.3	MATHCAD	32114423131114
Задание 3.5	1553131531	#ЗНАЧ!

Аргументы функции

ЛОЗУНГ

Слово: ЗАЧЕТ

Ключ: "СЕССИЯ"

Значение: ГСЦБР

Рисунок 8. Другие пользовательские функции для исторических шифров

Получается макросы могут использоваться для создания интерактивных заданий и упражнений, демонстрации алгоритмов шифрования и дешифрования, а также для проведения различных симуляций, что может значительно облегчить процесс обучения и помочь студентам лучше понять принципы криптографии.

Использование Excel в обучении историческим шифрам в криптографии может быть полезным и эффективным. В целом, использование Excel в обучении историческим шифрам в криптографии предоставляет студентам удобные инструменты для анализа, визуализации и расшифровки шифров. Он помогает систематизировать данные, проводить математические операции, автоматизировать задачи и облегчает коллаборативную работу. Это позволяет студентам более эффективно изучать исторические шифры и развивать свои навыки в области криптографии.

Заключение

Таким образом, объединение педагогики и криптографии может привести к разработке эффективных методов обучения защите информации.

Методы активного обучения формируют умения и навыки у студентов, так же обеспечивает выполнения задач в процессе решения, которых они самостоятельно овладевают умением и навыками. Для этого можно использовать MS Excel.

Учебный процесс должен быть интересным и результативным. Применение активных методов позволит повысить уровень профессиональной подготовки и сделает этот процесс более увлекательным и продуктивным.

Все вышесказанное, позволит подготовить квалифицированных специалистов, которые смогут успешно применять криптографические технологии в практической деятельности и обеспечивать надежную защиту информации в современном цифровом мире.

Список литературы

1. Анашкина И.В. Активные и интерактивные формы обучения: методические рекомендации / Тамбов: Изд-во ООО Орион, 2011. 39 с.
2. Зарукина Е. В., Логинова Н. А., Новик М. М. Активные методы обучения: рекомендации по разработке и применению. Учеб.-метод. пособие/ СПб.: СПбГИЭУ, 2010. 59 с.
3. Зуфарова А.С. Роль информационных технологий в образовательном процессе // Управление образованием: теория и практика 2020 № 3 (39) С.105-114.
4. Зуфарова А.С. Роль технологии визуализации в учебной информации // Современное педагогическое образование. 2020 № 9 С. 39-41.
5. Кашапов М.М. Неимитационные методы обучения: методические указания / Ярослав. Гос ун-т, Ярославль. 2001. 32 с.
6. Курьянов М.А., Половцев В.С. Активные методы обучения: метод. пособие / Тамбов: Изд-во ФГБОУ ВПО«ТГТУ», 2011. 80 с.
7. Кыстаубаева К. Т. Интерактивные методы обучения на уроках информатики как одно из средств развития обучающихся // Инновационные педагогические технологии: материалы Междунар. науч. конф. . (г. Казань, октябрь 2014 г.) Казань: Бук, 2014. С. 272-274.
8. Минюк Ю.Н. Метод проектов как инновационная педагогическая технология // Инновационные педагогические технологии: материалы Междунар. науч. конф. (г. Казань, октябрь 2014 г.). Казань: Бук, 2014. С.6-8.
9. Сдвижков О.А. Основы математической логики и криптографии. Практикум в Excel. (Бакалавриат). Учебное пособие / КноРус, 2024. 356 с.

Creation of active methods of cryptography training using MS Excel

Anna S. Zufarova

Senior lecturer of the Department of "Higher mathematics"
Pacific State University
Khabarovsk, Russia
006694@pnu.edu.ru
ORCID 0000-0000-0000-0000

Yulia S. Buzykova

Associate Professor of the Department of MOSIT
MIREA-Russian Technological University
Moscow, Russia
juliaserg_buz@mail.ru
ORCID 0000-0000-0000-0000

Received 20.01.2024

Accepted 20.02.2024

Published 15.03.2024

UDC 004.492:51:681.3

DOI 10.25726/b8190-7254-5061-f

EDN OKGVEQ

VAK 5.8.2. Theory and methodology of teaching and upbringing (by fields and levels of education) (pedagogical sciences)

OECD 05.03.HE EDUCATION, SPECIAL

Abstract

At the present time, there are problems of improving the quality of domestic education, in this regard, it is necessary to improve not only information technology, technical support, but also educational technologies. Modern needs for highly professional specialists in the field of information security cannot be realized without restructuring the system of professional training. Because of this, it is necessary to introduce active teaching methods into the educational process. The relevance of this topic is due to the fact that the study of historical ciphers is an integral part in the study of cryptographic methods of information protection. Studying historical ciphers using MS Excel allows you to analyze large amounts of data and makes it easier to work with numeric and textual data. This product is designed for creating tables, various calculations, data visualization and charting, and much more, which makes it a useful tool for learning the basics of cryptography. In the study of historical ciphers, MS Excel allows researchers to analyze the frequency of letters, words and bigrams, perform various mathematical operations to decrypt texts, and create statistical models for analyzing ciphers. Also, using this application, you can use custom functions and macros to automate solutions to classic cryptography problems. This contributes to the quality of teaching students the basics of cryptography. Due to its popularity and ease of use, MS Excel can become a popular tool in the research of historical ciphers, data analysis and teaching the basics of cryptography. Its application is also of great relevance in modern cryptography research, for example, RSA, the Diffie-Hellman protocol.

Keywords

active learning methods, simulation learning methods, non-simulation learning methods, exercises, cryptography, cipher, historical ciphers, Caesar cipher, information security, user functions, macros, MS Excel.

References

1. Anashkina I.V. Active and interactive forms of learning: methodological recommendations / Tambov: Publishing house of Orion LLC, 2011. 39 p.
2. Zarukina E. V., Loginova N. A., Novik M. M. Active learning methods: recommendations for development and application. Study method. the manual/ St. Petersburg: SPbSUE, 2010. 59 p .
3. Zufarova A.S. The role of information technologies in the educational process // Education management: theory and practice 2020 No. 3 (39) pp.105-114.
4. Zufarova A.S. The role of visualization technology in educational information // Modern pedagogical education. 2020 No. 9, pp. 39-41.
5. Kashapov M.M. Non-imitation teaching methods: methodological guidelines / Yaroslav. State University, Yaroslavl. 2001. 32 p.
6. Kuryanov M.A., Polovtsev V.S. Active teaching methods: method. manual / Tambov: Publishing house of FGBOU VPO"ТSTU", 2011. 80 p.
7. Kystabaeva K. T. Interactive teaching methods in computer science lessons as one of the means of developing students // Innovative pedagogical technologies: materials of the International Scientific Conference (Kazan, October 2014) Kazan: Buk, 2014. pp. 272-274.
8. Minyuk Yu.N. Project method as an innovative pedagogical technology // Innovative pedagogical technologies: materials of the International Scientific Conference (Kazan, October 2014). Kazan: Buk, 2014. pp.6-8.
9. Sdvizhkov O.A. Fundamentals of mathematical logic and cryptography. A workshop in Excel. (Bachelor's degree). Textbook / KnoRus, 2024. 356 p.