

education provide students with the opportunity to improve their skills and gain professional competence through virtual mobility. Virtual mobility, along with the knowledge acquisition, creates a potential for the international experience gaining by students and teachers, promotes international communications and develops intercultural communication skills through the students cooperation of various cultural backgrounds. Keywords: virtual mobility, distance education, academic mobility, information technology, intercultural communication, learning.

УДК 378.147.227

К ВОПРОСУ О ВЛИЯНИИ КОМПЬЮТЕРНЫХ ТЕХНОЛОГИЙ НА КАЧЕСТВО ОБУЧЕНИЯ СТУДЕНТОВ РАДИОТЕХНИЧЕСКИХ СПЕЦИАЛЬНОСТЕЙ

Курочкин А.Е.

Учреждение образования «Белорусский государственный университет информатики и радиоэлектроники»

Аннотация. Обращается внимание на роль математики, как фундаментальной науки, основы для формирования академических и профессиональных компетенций будущего инженера. Отмечаются низкие базовые математические знания студентов третьего курса радиотехнической специальности. Указывается на необходимость оптимального сочетания классических и инновационных методов обучения.

Ключевые слова: качество и уровень знаний, инновационные методы, компьютерные технологии, учебный процесс.

Внедрение компьютерных технологий в учебный процесс школ и высших учебных заведений настолько овладело нашим менталитетом, что порой забываются конечные цели, ради которых эти технологии и предназначены. Благородна цель: освободить серое вещество обучаемых от ручного решения математических задач в пользу решения более сложных задач с помощью компьютера. Хороший аргумент в пользу применения современных программных продуктов. Конечно, они позволяют одним нажатием клавиши превратить решение любой сложной задачи в приятную прогулку за чашкой кофе! Когда кофе будет выпито, то задача уже будет решена. Развитие вычислительных инструментов всегда было направлено на ускорение этапа расчётов в процессе создания общественно полезного продукта. Несомненно, это то, что требуется для развития у будущих инженеров необходимых на современном этапе навыков и компетенций. Но, что мы получаем на практике?

Школьники, выросшие в пору расцвета интернета, прекрасно знают о существовании “решебников” (слово-то какое придумано!) буквально по всем дисциплинам. Но какая может быть польза от копирования готового результата. Любопытные, возможно, попытаются разобраться с ходом решения задачи, но подробные объяснения должны даваться на школьных уроках, а не в интернете. Основная же масса учеников просто переписывает текст решения, не вдаваясь в подробности и не проверяя полученные ответы. А ошибки там встречаются в огромном количестве. Ведь порой эти самые “решебники” и пишут сами ученики.

Далее, учитывая полученный “школьный опыт”, бывшие школьники уже в статусе студентов высшего учебного заведения повторяют свои действия по отработанному сценарию при формировании отчётов в рамках различных форм текущей аттестации. В частности оформление пояснительной записки к типовому курсовому проекту или отчёта по лабораторной работе сводится к подстановке данных в компьютерную программу, написанную кем-то на MathCAD и выложенную в интернете, и распечатке текста на принтере. Всё сводится к нескольким нажатиям на клавиши компьютерной клавиатуры. В результате получаем откровенный плагиат порой с грубейшими опечатками, банальными

орфографическими и синтаксическими ошибками. Самостоятельные формы работы студентов в течение семестра, к сожалению, пока себя не оправдывают.

Автор этих строк на практических и лабораторных занятиях по дисциплине Радиоприёмные устройства неоднократно отмечал примечательный факт. Студенты третьего курса дневной формы обучения, как оказалось, в основной своей массе уже не умеют пользоваться ручкой и бумагой для выполнения арифметических операций. На это обстоятельство обращалось внимание в [1,2]. И просто пугает история с извлечением квадратных корней на одном из занятий. В ходе решения задачи надо было определить уровень сигнала U на сопротивлении $R = 8$ Ом, приводящий к выделению мощности на нём $P = 0,05$ Вт. Как известно, $P = U^2/R$, откуда следует, что $U = (P \cdot R)^{0,5} = (0,05 \cdot 8)^{0,5} = (0,4)^{0,5}$. Многие, посчитав в уме, быстро давали ответ 0,2!

Ну и просто катастрофической выглядит ситуация в группах студентов заочной формы обучения. Есть опасение, что и таблица умножения многими уже давно забыта.

К большому сожалению, для решения даже примитивных математических задач студенты используют калькуляторы. Полученным результатам они доверяют, даже не пытаясь произвести проверку каким-то другим способом. Но полностью доверяться компьютеру нельзя. При использовании чисел с плавающей запятой в формате *double* длина мантиисы составляет 52 двоичных разряда, что соответствует 16-ти верным знакам мантиисы после десятичной запятой. Последний знак мантиисы, как правило, не является точным. В результате вычитание соизмеримых чисел вызывает очень большие погрешности.

Особенно важно учитывать эту особенность компьютера при использовании разложения в цепную дробь. В качестве примера в таблице 1 представлены результаты разложения функции входного сопротивления лестничного фильтра двадцатого порядка ($n=20$). Видно как происходит постепенная потеря точности расчёта параметров в процессе разложения из-за того, что данные на каждой итерации используются для вычисления всех последующих значений. Значение для параметра g_1 получается с большей точностью, а все последующие значения g_n получаются с меньшей точностью.

Знаки, заслуживающие доверия, в таблице выделены жирным шрифтом. Одна итерация увеличивает число ненадёжных знаков примерно на одну единицу. В результате для 16 знаков мантиисы (стандартная компьютерная математика) синтез фильтра 20-го порядка оказывается невозможным. О потере точности расчётов говорит и появление в процессе разложения коэффициентов с отрицательными значениями.

Таблица 1. Коэффициенты функции входного сопротивления

g_n	Длина мантиисы m , знаков			
	16	18	12	10
g_1	0.2954195543744352	0.29541955437444	0.295419554374	0.2954195544
g_2	0.7134611095649473	0.71346110956499	0.713461109561	0.7134611098
g_3	1.0058241561837966	1.00582415618413	1.005824156152	1.0058241581
g_4	1.077852713500736	1.07785271350291	1.077852713286	1.0778527266
g_5	1.3444551271936078	1.34445512721384	1.344455125133	1.3444552542
g_6	1.111684255891377	1.11168425601542	1.111684243014	1.1116850547
g_7	1.7143743392240474	1.71437434115213	1.714374137835	1.7143868615
g_8	0.9418886557877248	0.94188866449494	0.941887744902	0.9419453415
g_9	2.363283639323256	2.36328390591041	2.363255746937	2.3650210613

g_{10}	0.6862859767247607	0.68628661828577	0.686218857231	0.6904969103
g_{11}	3.431429449037259	3.43147128394913	3.427058873063	3.7323116007
g_{12}	0.4726561909475649	0.47270397320746	0.467724626061	2.4216582208
g_{13}	4.709377926992177	4.71519519287878	4.183521806709	-0.0157276474
g_{14}	0.3428356584472274	0.34636667160111	0.19113105171	-1.8857040979
g_{15}	5.5519951966932135	6.20632346322519	1.869831540234	5.4401419765
g_{16}	0.266596319236514	92.8313518646038	0.219631316503	0.3362139249
g_{17}	5.082558302126313	-0.00000492164538	5.527060239925	5.8435977804
g_{18}	0.1610284249850325	-92.50550539104933	0.270098171961	0.272047304
g_{19}	2.776428788285468	6.44373312115062	5.803602803799	5.8088384512
g_{20}	0.1015547775683366	0.19975360242714	0.196154248425	0.196187588

Преодолеть ограничения стандартного компьютерного представления данных можно, используя специальные алгоритмы, позволяющие выполнять математические операции над числами с произвольной длиной мантииссы. Именно для этого и нужны современные технологии, позволяющие всем обучаемым радиотехнических специальностей создавать свои простейшие программные продукты, которым можно доверять при проведении радиотехнических расчётов любой сложности. При обработке чисел с плавающей запятой довольно часто требуются размеры мантииссы выше аппаратно допустимых норм. А для этого не следует забывать такие “скучные” школьные уроки математики, на которых осуществлялось выполнение простейших арифметических операций “в столбик”.

В таблице 2 представлены результаты расчёта с помощью разработанной программы, умеющей работать с длинными мантииссами. Достоверные знаки по-прежнему выделены жирным шрифтом.

Таблица 2. Коэффициенты функции входного сопротивления при “длинных” вычислениях с повышенной разрядностью

g_n	Число знаков мантииссы, m	
	35	20
g_1	0.29541955437443521234270754113370597	0.29541955437441918125
g_2	0.71346110956494770514221366391859639	0.71346110956492562165
g_3	1.00582415618379906860783798845944071	1.00582415618376512004
g_4	1.07785271350076178568663714200750203	1.07785271350075846525
g_5	1.34445512719388538671280141702242219	1.3444551271938227563
g_6	1.11168425589288948820596037242747494	1.11168425589293352591
g_7	1.71437433924616586808365116126544162	1.71437433924599381954
g_8	0.94188865588618165813373786619549812	0.94188865588630104095
g_9	2.36328364232728559753138888157461324	2.36328364232697440206
g_{10}	0.68628598394432447400787491979955783	0.68628598394490111828
g_{11}	3.43142991972162246337327736981691306	3.43142991974727706806
g_{12}	0.47265672846545710665015125692951756	0.47265672849624487801
g_{13}	4.70944327943090841876418474018773942	4.70944328315065456257
g_{14}	0.34287486784923316429063186125006768	0.34287487008270803596
g_{15}	5.5584212794644475922170926162725545	5.55842164595773737713
g_{16}	0.26889102543877707002874336014120063	0.26889115763191673432

g_{17}	5.38926356750380907501118635766229738	5.38928251451168597175
g_{18}	0.20116483123675980824844619535676139	0.20116820111059881736
g_{19}	3.56730554782473862267980868539358304	3.56744282237718140891
g_{20}	0.05908391087488704086303198313051947	0.0590804065438504839

Следует отметить, что стандартное приложение операционной системы Windows «Калькулятор» в инженерном режиме вычисляет с точностью до 32 значащих цифр. Этого значения в рассматриваемом случае (для $n = 20$) всё равно не хватает для получения 16-ти точных цифр, заслуживающих полного доверия, а тем более в случаях $n > 20$.

Следует обращать внимание студентов на указанную проблему в случае применения компьютеров и микроконтроллеров с низкой разрядностью, при создании криптографических проектов для систем шифрования данных, а также систем цифровой подписи, где используют целочисленную арифметику с очень большими положительными натуральными числами. Финансовое программное обеспечение также требует, чтобы результат вычисления на компьютере совпал до последнего разряда с результатом вычисления на бумаге. Для исключения грубых ошибок студенты должны уметь правильно оценивать последствия применения популярных компьютерных технологий в реальных задачах.

Заключение.

1. Необходимо повысить уровень и активизировать процесс математического образования студентов младших курсов до изучения специальных технических дисциплин.

2. На учебных занятиях необходимо обращать внимание студентов на практическую полезность и необходимость применения компьютерных технологий для решения сложных задач там, где без них трудно обойтись. По возможности следует стараться обойтись традиционными методами. Необходимо добиться оптимального сочетания классических и инновационных методов решения поставленных задач в учебном процессе.

3. При выполнении курсовых проектов и лабораторных работ должен соблюдаться принцип - инновации не в ущерб качеству. Нужен более жёсткий контроль работы студентов над черновыми вариантами пояснительных записок и отчётов, причём только в рукописном виде.

Список литературы:

1. Метельский, А.В. О математическом образовании студентов инженерных специальностей / А. В. Метельский, Е. А. Федосик, Н. И. Чепелев // Высшее техническое образование: проблемы и пути развития : материалы VIII Междунар. науч.-метод. конф. (Минск, 17–18 ноября 2016 года). В 2 ч. Ч. 2 / редкол. : Е. Н. Живицкая [и др.]. – Минск : БГУИР, 2016.– С. 62-66.

2. Майсеня, Л.И. Проблемное поле модернизации математического образования студентов технических университетов / Л. И. Майсеня // Высшее техническое образование: проблемы и пути развития : материалы VIII Междунар. науч.-метод. конф. (Минск, 17–18 ноября 2016 года). В 2 ч. Ч. 2 / редкол. : Е. Н. Живицкая [и др.]. – Минск : БГУИР, 2016.– С. 26-30.

ON THE QUESTION OF THE INFLUENCE OF COMPUTER TECHNOLOGIES ON QUALITY OF STUDENTS TEACHING OF RADIO-TECHNICAL SPECIALTIES

Kurochkin A.E.

Belarusian state university of informatics and radioelectronics

Abstract. Draws attention to the role of mathematics, as a fundamental science, the basis for the formation of academic and professional competencies of the future engineer. Low basic mathematical knowledge of third-year students of radio engineering specialty is

noted. It points to the need for an optimal combination of classical and innovative teaching methods

Key words: quality and level of knowledge, innovative methods, computer technologies, educational process

УДК 004.056.55

ФОРМИРОВАНИЕ ТЕМАТИКИ ДИСЦИПЛИНЫ «КРИПТОГРАФИЧЕСКАЯ ЗАЩИТА ИНФОРМАЦИИ»

Кутьин М.К., Дубовик А.А.

Военная академия Республики Беларусь

Аннотация. В статье рассматривается формирование тематики учебной дисциплины «Криптографическая защита информации» в интересах подготовки специалистов по противодействию использованию информационно-коммуникационных технологий в противоправных целях в условиях многообразия предметной области при ограниченном объеме учебного времени.

Ключевые слова: криптографическая защита информации, шифрование, аутентификация, протокол, учебная дисциплина.

В настоящее время в условиях динамично развивающихся информационно-коммуникационных технологий особую актуальность приобретают две противоположных по целям, но находящихся в постоянном взаимосвязанном развитии, области знаний – защита информации и вскрытие информации.

Все возрастающее значение защиты информации, циркулирующей в различных каналах связи, в системах управления, обуславливается тем, что кибератакам, взлому серверов, вмешательству в функционирование систем управления в настоящее время придается статус элементов гибридной войны. Последствия кибератак для государств могут оказаться много серьезнее, чем последствия силового военного воздействия. Здесь в качестве возможных последствий необходимо рассматривать финансовый и энергетический кризисы, управленческий хаос, транспортный коллапс и другие.

Непрерывно совершенствующиеся технологии защиты информации используются как во благо общества, так и в противоправных целях, когда общедоступные защищенные каналы связи применяются террористами для передачи преступной информации. Именно в связи с этим, в целях предотвращения преступных замыслов возникает насущная необходимость вскрытия защищенной информации. Это обуславливает непрерывное развитие и совершенствование технологий вскрытия защищенной информации.

Защиту информации и вскрытие информации можно рассматривать как обширные области научных знаний, применение которых требует подготовки специалистов с высокой квалификацией. С другой стороны, защиту информации и вскрытие информации можно рассматривать как философские категории единство и борьба противоположностей.

В связи с этим, очевидным становится тезис о том, что при подготовке специалистов по вскрытию информации необходимо глубокое изучение технологий защиты информации.

В настоящее время в области защиты информации выделяют три основных направления:

- организационные мероприятия по защите информации;
- аппаратные средства и способы защиты информации;
- криптографическая защита информации (КЗИ).

Наибольшую эффективность, максимальный вклад в защиту информации приносят криптографические методы защиты. Именно поэтому, в учебных планах подготовки специалистов по защите информации в различных ВУЗах обязательно