

Л. В. Котова,
Московский педагогический государственный университет

ЛАБОРАТОРНЫЕ ИССЛЕДОВАТЕЛЬСКИЕ РАБОТЫ В ПРОФЕССИОНАЛЬНО НАПРАВЛЕННОМ ОБУЧЕНИИ МЕТОДАМ И СРЕДСТВАМ ЗАЩИТЫ ИНФОРМАЦИИ БУДУЩИХ БАКАЛАВРОВ ПЕДАГОГИЧЕСКОГО ОБРАЗОВАНИЯ

Аннотация

В статье рассмотрены роль и место лабораторных исследовательских работ как средства реализации профессиональной направленности обучения математике будущих учителей информатики при изучении методов и средств защиты информации. Уточнено определение лабораторной исследовательской работы. Выделены цели и задачи лабораторных исследовательских работ по криптографии. Описаны их содержательное и технологическое обеспечение, организационные условия их проведения. Представлена разработка лабораторных исследовательских работ по криптографии в рамках модульного подхода к конструированию содержания. Приведены примеры задач, которые могут быть полезны для повышения эффективности математической подготовки школьников.

Ключевые слова: интегрированный курс, профессиональная направленность обучения, проблемное обучение, профессионально ориентированная самостоятельная поисковая деятельность, лабораторная исследовательская работа.

При организации учебной деятельности будущего учителя информатики в рамках его профессионально ориентированной математической подготовки одним из важнейших элементов является вовлечение студентов в работу с изучаемым материалом, что становится возможным только при продуманном использовании всевозможных видов самостоятельной и исследовательской работы. Только в результате самостоятельного решения задач, требующих для решения привлечения знаний и умений из различных областей науки, у будущего учителя может сформироваться представление о научной картине мира, роли ранее изученных дисциплин в решении прикладных задач и возможностях использования теоретических знаний в будущей профессиональной деятельности.

Большую роль здесь могут сыграть *междисциплинарные и интегрированные курсы* — база для формирования общей и профессиональной культуры, быстрой адаптации к новым специализациям,

теоретическая основа широкого развертывания прикладных разработок.

К таким интегрированным дисциплинам, сочетающим в себе *фундаментальную, прикладную, педагогическую и социально-культурную составляющие*, мы относим дисциплину «Методы и средства защиты информации» (МСЗИ), предназначенную для студентов направления подготовки «Педагогическое образование», профили подготовки: «Информатика», «Информатика и математика», «Математика и информатика», «Информатика и экономика». Дисциплина входит в вариативную часть профессионального цикла ООП бакалавриата (7-й, 8-й или 9-й семестр) и направлена на формирование всех компетенций, имеющих отношение к уровню *математической подготовки будущих учителей информатики*. УМК дисциплины разработан и апробирован на кафедре теории чисел Московского педагогического государственного университета.

Контактная информация

Котова Лидия Владимировна, ст. преподаватель кафедры теории чисел математического факультета Московского педагогического государственного университета; адрес: 119991, г. Москва, ул. Малая Пироговская, д. 1, стр. 14; телефон: (499) 264-25-56; e-mail: kolv@inbox.ru

L. V. Kotova,
Moscow State Pedagogical University

LABORATORY RESEARCH WORKS IN PROFESSIONALLY DIRECTED TRAINING TO METHODS AND MEANS OF INFORMATION PROTECTION OF FUTURE BACHELORS OF PEDAGOGICAL EDUCATION

Abstract

The article describes the role and place of laboratory research works as means of realization of a professional orientation of training future informatics teachers to mathematics while studying methods and means of information protection. The definition of laboratory research work has been clarified. The goals and tasks of laboratory research work on cryptography are singled out. Their informative and technological support, organizational conditions for their conduct are described. The laboratory research works on cryptography within the framework of a modular approach to the design of content are presented. Examples of tasks that can be useful for improving the efficiency of mathematical teaching of schoolchildren are given.

Keywords: integrated course, professional orientation of teaching, problem training, professionally oriented independent search activity, laboratory research work.

Для освоения дисциплины студенты используют знания и умения, сформированные в процессе изучения *фундаментальных* предметов математического и естественнонаучного цикла, в частности, знания по *алгебре* (матрицы и определители, свойства делимости в кольце полиномов над полем); *теории чисел* (теория сравнений, функция Эйлера, первообразные корни, цепные дроби); *основам программирования* (вычислительные алгоритмы, навыки программирования в системах Borland C++, Java). Таким образом, дисциплина МСЗИ является частью *фундаментальной математической подготовки* студентов-информатиков и *интегрированным курсом*, реализующим принцип непрерывности и преемственности, выявляющим междисциплинарные связи как внутри математики, так и между смежными дисциплинами — математикой и информатикой.

Содержание дисциплины формируется из различных тематических модулей, которые можно варьировать в соответствии с целями обучения, профильной направленностью и уровнем предварительной подготовки студентов. Разработанные нами тематические модули — *базисные* (Б), *вариативные* (В) и *дополнительные* (Д) — позволяют организовать профессионально ориентированное изучение дисциплины МСЗИ, конструируя и реализуя для различных профилей различные схемы обучения.

Для дисциплины МСЗИ разработаны *пять базисных тематических модулей*:

- (М1) исторические аспекты развития криптографии;
- (М2) математические основы шифрования и простейшие криптосистемы;
- (М3) шифрующие матрицы;
- (М4) современные средства защиты информации, новые направления, система RSA;
- (М7) факторизация натуральных чисел.

Для различных профилей предлагаются *три вариативных модуля*:

- (М5) временные оценки сложности арифметических операций;
- (М6) простые и псевдопростые числа;
- (М8) псевдослучайные последовательности и их применение в криптографии.

В случае недостаточной теоретической готовности студентов им может быть предложен *дополнительный вспомогательный модуль* (М0), содержащий необходимые теоретические сведения из теории чисел и алгебры.

Для студентов, имеющих вторым профилем социально-экономический, может быть предложен *дополнительный экономический модуль* (МЭ), рассматривающий прикладные задачи данной тематики.

Основываясь на анализе конкретных условий и задач, возникающих при изучении нашей предметной линии, учитывая специфику обучения студентов различных профилей, мы выделили следующие **критерии выбора методов обучения для тематических модулей**, требующие их соответствия:

- общим целям профессионально направленной подготовки будущих учителей информатики;
- особенностям изучаемой дисциплины в целом;
- целям, задачам и содержанию конкретного модуля;

- времени, отведенному на изучение модуля; уровню математической подготовки и навыкам программирования студентов;
- профилю подготовки;
- материальной оснащенности учебного заведения;
- методическому сопровождению в виде пособий и средств удаленного контроля.

Используя при реализации дисциплины МСЗИ все классические методы обучения (словесный, объяснительно-иллюстративный, практический, наглядный, репродуктивный, эвристический, исследовательский и т. д.), мы, прежде всего, опирались на возможности **проблемного метода обучения**.

Теория проблемно-развивающего обучения представлена в трудах М. И. Махмутова, Ю. К. Бабанского, Т. В. Кудрявцева, И. Я. Лернера, Дж. Брунера, В. Оконь, Т. Новацкого, Х. Век и др. Цель проблемного обучения — усвоение не только результатов научного познания, но и самого пути, процесса получения этих результатов (овладение способами познания). Это отвечает задачам нашей дисциплины: современность подавляющего большинства вопросов, рассматриваемых в рамках МСЗИ, требует особое внимание уделять не решенным задачам, а открытым практическим проблемам и теориям, которые разрабатываются для их решения.

В российской педагогике различают *три основные формы проблемного обучения* [8]:

- проблемное изложение учебного материала в монологическом режиме лекции либо диалогическом режиме семинара;
- частично-поисковая деятельность;
- самостоятельная исследовательская деятельность.

Все эти формы мы реализуем в ходе образовательного процесса на *лекциях* (форма 1), *семинарах* (формы 1 и 2) и *лабораторных исследовательских работах* (формы 2 и 3).

Под **лабораторными работами** понимают один из видов самостоятельной практической работы, проводимой учащимися с целью углубления и закрепления теоретических знаний, развития навыков самостоятельного экспериментирования [1].

Лабораторная работа подразумевает:

- изучение определенного процесса на практике с использованием при этом методов, предварительно изученных на лекциях;
- выбор наиболее оптимального приема выполнения, приема исследования, которые обеспечивают наиболее точный результат;
- определение фактического результата и его сравнение с теоретическими данными;
- обнаружение причин полученного соответствия или несоответствия с теоретическими результатами;
- формулирование в отчете лабораторной работы собственных выводов, сделанных на основе полученных результатов.

В этом смысле лабораторная работа по математике и информатике мало отличается от привычного понимания лабораторной работы по физике, химии и т. д.

В условиях нашей дисциплины выполнение лабораторных работ позволяет студентам:

- овладеть навыком математического моделирования;
- овладеть навыком поиска методов решения поставленных задач в междисциплинарных областях;
- выявить практическую значимость теоретических сведений, полученных ранее;
- научиться оценивать эффективность найденных методов решения задач;
- получить опыт исследовательской деятельности;
- ознакомиться с методами организации учебно-исследовательской работы.

Для нашего исследования принципиально важно, что лабораторные работы в рамках интегрированных математических курсов могут выполнять и функции профессионально ориентированной самостоятельной поисковой деятельности (ПО СПД) студентов, направленной на переработку профессионально значимой информации, проектируемой и реализуемой в профессионально заданных ситуациях [9].

Поэтому при изучении МСЗИ мы говорим об использовании лабораторных исследовательских работ (ЛИР), совмещающих возможности лабораторных работ и ПО СПД.

Под лабораторной исследовательской работой в рамках изучения дисциплины МСЗИ мы понимаем организуемую педагогом самостоятельную деятельность студентов, направленную на реализацию, анализ и поиск оптимизации алгоритмов, выбор и применение приёмов научных методов познания при решении профессионально значимых задач.

Цели (Ц) и задачи (З) лабораторной исследовательской работы полностью соответствуют разработанным предметно-профессиональным компетенциям соответствующего модуля и дисциплины в целом и имеют теоретические (Т), прикладные (П) и общепрофессиональные (ОП) аспекты:

- для Т-целей характерны требования «ознакомиться», «изучить соответствующую теорию, метод» и т. д.;
- для П-целей — «реализовать алгоритм», «рассмотреть приложения теории к решению задачи» и т. д.;
- для ОП-целей — «определить возможность применения изученного к последующей профессиональной деятельности».

Содержательное обеспечение (СО) лабораторной исследовательской работы представлено программой дисциплины, учебными пособиями и электронным курсом:

- В программе дисциплины [6] выделены компетенции обучающегося, формируемые в результате освоения дисциплины, представлено тематическое планирование, приведены примеры заданий для различного вида работы по дисциплине, в том числе для лабораторных работ.
- Сборник задач по дисциплине [7] имеет как печатный, так и электронный вид в университетской библиотеке. Он предназначен для

использования на семинарских занятиях и лабораторных работах.

- Учебное пособие «Теоретико-числовые основы защиты информации» содержит теоретический материал и задачи различного уровня сложности из области криптографии и прикладных вопросов теории чисел. Пособие полностью обеспечивает теоретическим материалом все лабораторные работы дисциплины МСЗИ [4].
- Электронный курс по основам криптографии, разработанный нами в системе Moodle, служит дополнением к имеющимся пособиям. Он позволяет совмещать учебные, развивающие и контролирующие функции обучения, предоставляет условия для удаленного выполнения лабораторных работ, упрощая систему обратной связи и контроля над работами студентов.
- Учебное пособие «Сборник задач по теории чисел» [3] содержит все необходимые теоретические факты из теории чисел, лежащие в основе криптографических задач.

В рамках **технического обеспечения (ТО) лабораторной исследовательской работы** студентами могут использоваться:

- интерактивная система MATLAB (The MathWork);
- компьютерная система Derive (Soft Warehouse Inc.);
- математический пакет Mathematica 2.2/.../4 (Wolfram Research Inc.);
- математическая система MathCAD 3.0/.../8.0 (MathSoft);
- электронные таблицы Microsoft Excel;
- системы программирования: Turbo Pascal, Borland C++, Java.

С точки зрения **организационных условий (ОУ)** мы считаем наиболее эффективной на ЛИР работу в малых группах (два-три человека), члены которых решают как общие, так и индивидуальные задания. Групповая форма деятельности учащихся стимулирует взаимодействие между членами группы, позволяет выстроить отношения взаимной ответственности и поддержки, повышая уровень самоконтроля учащихся и давая навыки организации подобных форм деятельности для будущей работы со школьниками. При этом состав групп непостоянен и отчет о проделанной работе индивидуален.

В рамках изучения дисциплины МСЗИ для каждого модуля с учетом его теоретической, прикладной и общекультурной составляющих нами разработаны 14 лабораторных исследовательских работ. Их список представлен в таблице.

Как показывают теоретические исследования и опыт практической работы, профессионально ориентированная самостоятельная поисковая деятельность студентов по переработке информации является разноуровневой, в зависимости от уровня знаний, умений и навыков обучающихся, а также уровня их самоорганизации и саморегуляции. Как правило, выделяют три уровня ПО СПД [9]:

- репродуктивно-поисковый (РП);
- поисково-исследовательский (ПИ);
- исследовательско-проектировочный (ИП).

Лабораторные исследовательские работы для дисциплины «Методы и средства защиты информации»

	Модуль	Лабораторные исследовательские работы
M1	Из истории криптографии	ЛИР № 1 «Старинные шифры и олимпиадные задачи»
M2	Некоторые простые криптосистемы	ЛИР № 2 «Простейшие криптосистемы»
M3	Шифрующие матрицы	ЛИР № 3 «Матричное шифрование»
M4	Новые направления. Система RSA	ЛИР № 4 «Система RSA и ее модификации»
		ЛИР № 5 «Дискретный логарифм»
M5	Временные оценки сложности арифметических операций	ЛИР № 6 «Оценка сложности простейших алгоритмов»
		ЛИР № 7 «Алгоритм Евклида, модификации, оптимизация»
		ЛИР № 8 «Решение неопределенных линейных уравнений»
M6	Простые и псевдопростые числа	ЛИР № 9 «Простые числа. Числа специального вида»
		ЛИР № 10 «Тесты на простоту»
M7	Факторизация натуральных чисел	ЛИР № 11 «Классические методы факторизации»
		ЛИР № 12 «Современные методы факторизации»
M8	Псевдослучайные последовательности и их применение в криптографии	ЛИР № 13 «Построение конечного поля»
		ЛИР № 14 «Построение псевдослучайной последовательности»

Учитывая разноуровневость ПО СПД и неоднородность контингента студентов, мы выделяем **четыре уровня заданий для ЛИР:**

- *репродуктивный (Р);*
- *репродуктивно-поисковый (РП);*
- *поисково-исследовательский (ПИ);*
- *исследовательско-проектировочный (ИП).*

Мы полагаем, что достигаемый студентом в ходе решения задач ЛИР уровень ПО СПД существенно зависит от всех дидактических составляющих: целевых, содержательных, организационных, технологических. Реализация такого подхода представлена на рисунках 1 и 2 на примере ЛИР № 12 «Современные методы факторизации».

Рассмотрим подробнее на примерах каждого модуля реализацию предложенного подхода.

Первый модуль М1 не требует специальной математической подготовки. Основу ЛИР по данному модулю составляют задачи олимпиад для школьников по математике и криптографии [2], которые проводятся с 1991 года. Обучающимся не требуются дополнительные технические средства, задания могут выполняться как индивидуально, так и в небольшой группе.

Основные цели изучения модуля М1, в частности, выполнения ЛИР в рамках этого модуля:

- изучить теорию построения классических криптосистем, методы криптоанализа; рассмотреть теоретические задачи, возникающие в связи с потребностью усовершенствования существующих криптосистем (Т-цели);
- продемонстрировать практическое применение материала разделов, изученных в курсах теории чисел и алгебры (П-цели);
- показать возможные направления для разработки школьных факультативных и внекласс-

ных занятий по математике и информатике (ОП-цели).

Примеры Т-заданий:

- Шифрование сообщения состоит в замене букв известного текста на пары цифр в соответствии с некоторой таблицей, в которой разным буквам алфавита соответствуют разные пары цифр. Определите, в каком случае будет легче восстановить текст: если известно, что первое слово второй строки — **ТЕРРИТОРИЯ**, или если известно, что первое слово третьей строки — **КОРРЕКТОР**.
- Какой сейф надежнее и почему? Первый содержит 100 переключателей по два положения в каждом; второй — восемь переключателей по 100 положений в каждом. Сейф открывается только при полном совпадении переключателей с кодовым значением.
- Рассмотрим преобразование цифрового текста, в котором каждая цифра заменяется остатком от деления значения многочлена $f(x) = a(x^3 + 7x^2 + 3x + b)$ на число 10, где a, b — фиксированные натуральные числа. Выясните, при каких значениях a и b указанное преобразование допускает однозначное расшифрование. (Данная задача школьной олимпиады может быть решена с использованием остатков от деления, однако при использовании простейших элементов теории сравнений решение существенно упрощается.)

Пример П-задания:

- Шифрование фразы на русском языке проходит в два этапа. На первом этапе каждая буква текста заменяется на следующую в алфавитном порядке (последняя заменяется на первую). На втором этапе применяется шифр простой

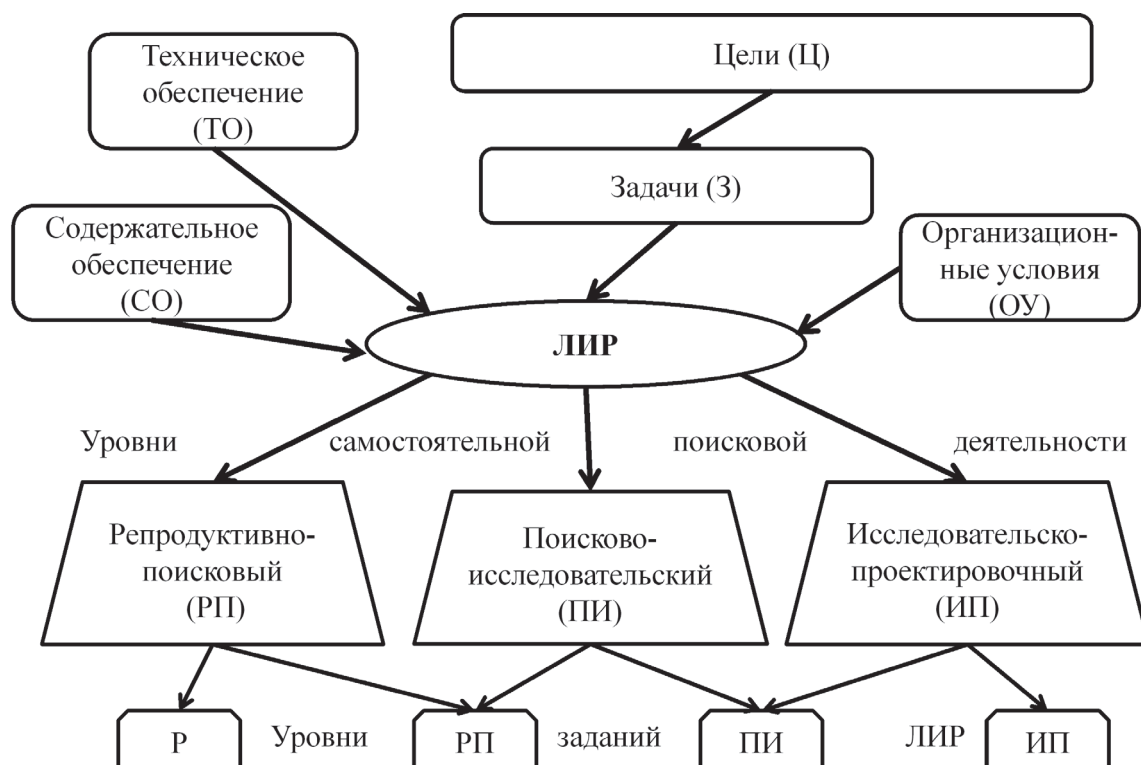


Рис. 1. Схема формирования уровней профессионально ориентированной самостоятельной поисковой деятельности в ходе лабораторной исследовательской работы



Рис. 2. Задания различного уровня профессионально ориентированной самостоятельной поисковой деятельности лабораторной исследовательской работы № 12

замены с неизвестным ключом. Его применение заключается в замене каждой буквы шифруемого текста буквой того же алфавита, при этом разные буквы заменяются разными буквами. По шифротексту: ГНПНВТ НРЗКЗС ЗГТШЗИ восстановите открытое сообщение, если известно, что результат шифрования не зависит от порядка выполнения этапов для любого открытого сообщения. Пробелы разделяют слова. (При решении этой задачи лучше всего воспользоваться таблицей Виженера.)

Примеры ОП-заданий:

- Составить шифротекст, полученный шифром простой замены, для вскрытия с использованием элементов частотного анализа.
- Составить решетку Кардано с недостающим элементом.

В данном случае задания направлены на подготовку будущих учителей к составлению задач для школьников при подготовке к олимпиадам по математике и криптографии.

Модули М2 и М3 условно можно назвать внутренними или вспомогательными. Они формируют математическую базу, необходимую для построения простейших криптосистем. Задания позволяют повторить, закрепить и расширить знания по теории чисел и линейной алгебре, а также увидеть приложения, которые можно использовать в школе для повышения познавательного интереса школьников. Задания лучше выполнять небольшими группами.

Выполнение лабораторных работ по материалу этих модулей позволит:

- изучить принцип работы симметричных криптосистем (Т-цели);
- продемонстрировать приложения изученных в теории чисел и алгебре разделов (П-цели);
- использовать полученные сведения для организации проектной деятельности школьников, для их подготовки к тематическим олимпиадам (ОП-цели).

Примеры Т-заданий:

- Найдите обратное аффинное преобразование для преобразования $f(P) \equiv AP + b \pmod{N}$ при $N = 30$, $A = 17$, $b = 2$. (*Репродуктивный уровень*.)
- Сколько существует различных линейных преобразований для N -буквенного алфавита? (*Репродуктивно-поисковый уровень*.)
- Говорят, что элемент P открытого текста неподвижен при данном шифрующем преобразовании, если $f(P) = P$. Пусть имеется линейное шифрующее преобразование N -буквенного алфавита. Докажите, что для четного N существуют, по крайней мере, две неподвижные буквы. (*Поисково-исследовательский уровень*.)

Пример ОП-задания:

- Перехвачено сообщение: «БХЗЭБЗКОХЖУА.ЩНЛК,Щ,Щ». При шифровании использовалось аффинное шифрующее преобразование букв 41-буквенного алфавита, включающего в себя буквы А—Я, имеющие числовые эквиваленты 0—32 соответственно, пробел = 33, далее: «., - ; : ! ; ?». Вам известно, что открытый текст заканчивается подписью «МАМА».

Прочитайте сообщение. Определите ключ шифрования и ответьте: «ПРИЕДУ ЗАВТРА». (*Поисково-исследовательский уровень*.)

Пример ОП-задания (задания школьных олимпиад по криптографии и математике):

- Каждую букву исходного сообщения заменили двузначным номером в русском алфавите таким образом, что А = 01, В = 02, ..., Я = 33. Полученную числовую последовательность разбили на трехзначные цифровые группы без пересечений и пропусков. Каждое из полученных трехзначных чисел умножили на 77 и оставили только три последние цифры произведения. В результате получилась последовательность: 317564404970017677550547850355. Восстановите сообщение. (*Исследовательско-проектировочный уровень*. При решении этой задачи школьникам (как и студентам) могли бы очень помочь начала теории сравнений.)

Модуль М4 знакомит студентов с современными криптосистемами и их модификациями, с современными правовыми и технологическими вопросами защиты информации. Изучение организации банковской системы защиты информации, действия электронных карт и электронной подписи способствует повышению интереса обучающихся к теории вопроса. Так как система RSA уже вошла в школьные учебники по информатике [5], то изучение модуля М4 реализует и профессиональную направленность курса МСЗИ.

В зависимости от условий проведения ЛИР и уровня готовности обучающихся работы могут проводиться и с элементами «ручного просчитывания», и с использованием вычислительных ресурсов, и с использованием самостоятельно созданных программ.

Выполнение лабораторных работ по материалу этого модуля позволит:

- изучить принцип работы асимметричных криптосистем (Т-цели);
- продемонстрировать действия изученных систем в современных повседневных реалиях (П-цели);
- использовать полученные сведения для освещения школьникам современных условий организации защиты информации, условий работы банковской сферы, а также обосновать степень защиты безналичных операций, занимающих все большее место в нашей повседневной жизни (ОП-цели).

Примеры Т-заданий:

- В системе «с открытым ключом» с модулем 259: а) найдите две различные пары ключей; б) укажите количество возможных пар шифрующих ключей (с учетом порядка). (*Репродуктивный уровень*.)
- Приведите пример неоднозначного дешифрования в системе «электронная подпись» при использовании неправильного порядка взятия ключей. (*Репродуктивно-поисковый уровень*.)
- Найдите такой модуль для системы «без передачи ключей», чтобы в качестве ключей можно было использовать числа: 3, 5, 7, 9, 11, 13, 15, 17, 19, 21. (*Поисково-исследовательский уровень*.)

Пример П-задания:

- Используя простые числа из заданного промежутка, создайте свой электронный адрес и ключи для работы в системе «электронная подпись». Передайте свой адрес и открытый ключ группе-напарнику. Получите у нее адрес и ключ. Возьмите в качестве сообщения число m меньше каждого из адресов, зашифруйте с помощью открытого ключа группы-напарника и своего секретного и передайте ей. Получите сообщение от группы-напарника, дешифруйте его. Сверьте полученные данные с данными группы-напарника. Подготовьте отчет о проделанной работе с обоснованием работы системы. (Поисково-исследовательский уровень.)

При выполнении этого задания студентами с различными дополнительными профилями будут смещаться смысловые акценты и самой работы, и отчета по ее выполнению:

- информатикам важна способность строить алгоритмы реализации криптографических систем;
- математикам следует уделить внимание математическому обеспечению таких систем;
- экономистов в первую очередь заинтересует принцип действия электронной подписи, реализуемый в банковской сфере.

Пример ОП-задания:

- Изучить доказательство теоремы Ферма на бусинах, предложенное американским математиком С. Голобом, и приготовить пошаговую презентацию этого доказательства для доступного изложения школьникам. (Исследовательско-проектировочный уровень.) (Это простое и красивое доказательство предлагалось в буклетах международного математического конкурса-игры «Кенгуру», вып. 3—2010.)

Модуль М7 знакомит с теоретико-числовыми проблемами, возникшими в связи с задачей вскрытия системы RSA. Для его изучения требуется предварительное знакомство с основными разделами теории чисел; необходимы и навыки программирования.

Выполнение лабораторных работ по материалу этого модуля позволит:

- изучить классические и современные алгоритмы разложения натуральных чисел на множители (Т-цели);
- продемонстрировать то, как использование классических идей наряду с развитием новых теорий помогает создавать алгоритмы, позволяющие решать задачи, возникающие с развитием новых технологий (П-цели);
- использовать полученные сведения для демонстрации школьникам на доступных их пониманию задачах важности получения новых знаний и развития новых теорий в математике для технологического прогресса (ОП-цели).

Примеры Т-заданий:

- Разложите число 1517 на множители известными вам классическими способами. (Репродуктивный уровень.)
- Подберите коэффициент из промежутка $[2; 10]$ для улучшенного метода Эйлера—Ферма, позволяющего факторизовать $N = 5\,338\,771$,

выполнив не более трех шагов (проверок). (Репродуктивно-поисковый уровень.)

- Выясните, простым или составным является число 629, рассмотрев представления этого числа в виде квадратичных форм. (Поисково-исследовательский уровень.)

Пример П-задания:

- Напишите программу, реализующую алгоритмы разложения чисел на множители. Исследуйте алгоритмы с точки зрения их результативности и эффективности в зависимости от вида числа (возьмите числа из промежутка от 10 000 до 10 050). В каких ситуациях предпочтительнее тот или иной метод разложения чисел на множители? (Поисково-исследовательский уровень.)

Пример ОП-задания:

- Сформулируйте доступные школьникам методы разложения натуральных чисел на множители (последовательного деления, комбинированный с поиском наибольшего общего делителя, метод Ферма), найдите четырехзначные числа, такие, что оптимальным для них будет только один метод. *Укажите составное четырехзначное число, «неудобное» для каждого из методов. (Исследовательско-проектировочный уровень.)

Вариативные модули М5, М6 и М8 имеют серьезную математическую составляющую и могут существенно расширить теоретические представления студентов о методах защиты информации, а также выступать в роле отдельных дисциплин по выбору. При этом с точки зрения профессиональной направленности подготовки будущих учителей информатики и математики задачи с простейшими арифметическими алгоритмами (М5), простыми числами (М6) и рекуррентными последовательностями (М8) могут быть адаптированы для школьников и послужить прекрасной базой для проведения урочной и внеурочной работы. Приведем примеры таких задач:

- Найдите НОД (1547, 560), используя разложение чисел на множители и алгоритм Евклида. Сравните трудоемкость этих способов (количество выполненных делений).
- Найдите НОД (1547, 560), используя алгоритм Евклида и бинарный алгоритм Евклида. Сравните временные затраты на работу этих алгоритмов.
- Используя расширенный алгоритм Евклида и расширенный бинарный алгоритм Евклида, найдите представление НОД (1547, 560) в виде линейной комбинации чисел 1547 и 560. Сравните процедуры по их трудоемкости.

При реализации этих алгоритмов на ЭВМ оценка трудоемкости (временных затрат) может быть получена непосредственно, при использовании функции оценки скорости алгоритма при многократном повторении его выполнения (иначе временные показатели слишком малы).

- Используя Решето Эратосфена, найдите все простые числа на отрезке $[1000; 1025]$.
- Найдите, какие остатки при делении на 12 могут давать квадраты простых чисел, больших 3.
- Решите в простых числах уравнение $y^2 = x^2 + 7$.

- Каким может быть произведение нескольких различных простых чисел, если оно кратно каждому из них, уменьшенному на 1?
- Для каждого простого p найдите наибольшую натуральную степень числа $p!$, на которую делится число $(p^2)!$.

Последние из представленных задач соответствуют олимпиадным задачам для школьников и задаче 19 вариантов ЕГЭ по математике.

- Найдите первые 10 членов рекуррентной последовательности $a_{n+1} = 2a_n + 1$, если $a_0 = 1$.
- Вычислите 15 первых членов псевдослучайной последовательности: $a_0 = 0$, $a_1 = 1$, $a_{n+1} = \text{rest}(a_n + a_{n-1}, 2)$.
- Сколько различных последовательностей, заданных уравнением $\delta_{x+4} = \delta_x + \delta_{x+1} + \delta_{x+2} + \delta_{x+3}$, может получиться, если первые четыре члена последовательности могут принимать только значения 0 и 1?

В заключение отметим, что опыт проведения ЛИР по дисциплине МСЗИ свидетельствует об эффективности данного вида деятельности для повышения интереса студентов-информатиков к математической составляющей их фундаментальной подготовки. Применение ранее изученного теоретического материала к решению современных прикладных задач и наглядная возможность его использования в по-

следующей профессиональной деятельности позволяют реализовать профессиональную направленность подготовки будущих учителей и формируют у них способность использовать знания о современной естественнонаучной картине мира в своей образовательной деятельности, готовность к непрерывному личностно-профессиональному росту.

Список использованных источников

1. Бим-Бад Б. М. Педагогический энциклопедический словарь. М., 2002.
2. Введение в криптографию / под общ. ред. В. В. Яценко. М.: МЦНМО, 2012.
3. Дега Е. И., Котова Л. В. Сборник задач по теории чисел. М.: URSS, 2011.
4. Дега Е. И., Котова Л. В. Введение в криптографию: Теоретико-числовые основы защиты информации // Основы защиты информации. № 14. М.: URSS, 2017.
5. Калинин И. А., Самылкина Н. Н. Информатика. 10–11 классы. Углубленный уровень. М.: БИНОМ. Лаборатория знаний, 2014.
6. Котова Л. В. Методы и средства защиты информации. Рабочая программа. М.: МПГУ, 2012.
7. Котова Л. В. Сборник задач по дисциплине «Методы и средства защиты информации». М.: МПГУ, 2015.
8. Махмутов М. И. Организация проблемного обучения в школе: книга для учителей. М.: Просвещение, 1977.
9. Рыблова А. Н. Технологически организованная профессионально ориентированная самостоятельная познавательная деятельность студентов // Педагогическое образование и наука. 2014. № 6.

НОВОСТИ

«Облачная» доля в расходах на ИТ-инфраструктуру растет все быстрее

По оценкам IDC, в 2017 году мировой объем закупок средств создания ИТ-инфраструктуры (серверов, корпоративных систем хранения и коммутаторов Ethernet) для применения в облачных средах составил 46,5 млрд долл., что на 20,9 % больше, чем в предыдущем году. Большая часть закупок (65,3 %) приходится на публичные облачные ЦОД. Этот сегмент рынка вырос за год на 26,2 %. Доля частных облачных сред на оборудовании провайдера составляет 13 %. При этом в расходах на частные облачные среды доля сред на собственном

оборудовании составляет 62,6 %. Мировой объем закупок средств для традиционной ИТ-инфраструктуры в 2017 году снизился на 2,6 % и составляет 57,2 % общего объема расходов конечных пользователей на продукты ИТ-инфраструктуры. В 2016 году он составлял 62,4 %. Доля его снижается быстрее, чем в последние три года, отмечают аналитики. Сегменты коммутаторов Ethernet и вычислительных платформ в 2017 году выросли соответственно на 22,2 % и 22,1 %, а сегмент систем хранения — на 19,2 %.

На защиту своих сетей российские компании выделяют 11 % ИТ-бюджета

Исследование уровня защищенности корпоративных сетей, проведенное компанией «Код безопасности», показало высокую востребованность встроенных в средства защиты механизмов мониторинга безопасности. Аналитиков в первую очередь интересовало, какие требования к средствам сетевой безопасности являются для заказчиков ключевыми. Для 67 % ИТ-руководителей и 77 % специалистов по информационной безопасности на первом месте по важности стоят стабильность работы и качественная техническая поддержка. 77 % организаций госсектора и 62 % учреждений здравоохранения назвали

приоритетным фактором российское происхождение решения. В среднем на защиту корпоративных сетей компании выделяют 11 % ИТ-бюджета, однако далеко не каждая компания направляет часть этих ресурсов на создание профильной структуры. Наибольшая доля компаний, имеющих выделенное подразделение сетевой безопасности, наблюдается в финансовой сфере (87 %) и промышленности (60 %). В среднем подобные структуры есть у 34 % компаний. В 4 % организаций госсектора и сферы здравоохранения сетевая безопасность передана на аутсорсинг.

(По материалам международного компьютерного еженедельника «Computerworld Россия»)