УДК 004:378.147:512.5

ОБ ИСПОЛЬЗОВАНИИ ИНФОРМАЦИОННЫХ ТЕХНОЛОГИЙ ПРИ ПРЕПОДАВАНИИ СОВРЕМЕННЫХ РАЗДЕЛОВ МАТЕМАТИКИ

ON THE USE OF INFORMATION TECHNOLOGIES IN THE TEACHING OF MODERN SECTIONS OF MATHEMATICS

Асмыкович И.К., Ловенецкая Е.И.,
Белорусский государственный технологический университет,
Минск, Беларусь

I.K. Asmykovich, E.I. Lovenetskaya,
Belarusian State Technological University, Minsk, Belarus

e-mail: asmik@tut.by

Аннотация. Статья посвящена анализу содержания и методического обеспечения курса «Математические основы криптографии» для студентов IT-специальностей. Подчеркивается, что в основе современных криптографических алгоритмов лежат теоретико-числовые и алгебраические структуры, включая группы точек эллиптических кривых над конечными полями.

Приведен краткий обзор существующих русскоязычных учебников и учебных пособий по математическим основам криптографии. Отмечается, что необходимыми компонентами курсов по математическим основам криптографии являются элементы теории чисел, модулярная арифметика, теория групп, колец и полей, понятие о построении и структуре конечных полей, а в последние годы также элементы теории эллиптических кривых.

Подробно описана по разделам программа курса, который читается в Белорусском государственном технологическом университете для студентов специальности «Программное обеспечение информационной безопасности мобильных систем». Особое внимание уделено электронному учебно-методическому комплексу (ЭУМК) по дисциплине «Математические основы криптографии». Описана его структура и содержание, показаны примеры оформления страниц и содержания электронного документа. Обсуждается методика преподавания этого курса с использованием ЭУМК и системы индивидуальных практических заданий по дисциплине.

Отмечена возможность научно-исследовательской работы студентов по данной тематике, перспективы расширения программы курса с учетом новейших достижений в криптографии. Обсуждаются возможности использования системы дистанционного обучения для методического обеспечения такой динамично изменяющейся дисциплины, какой в настоящее время является курс «Математические основы криптографии».

Abstract. The article is devoted to the analysis of the content and methodological support of the course “Mathematical foundations of cryptography” for students of IT specialties. It is emphasized that the basis of modern cryptographic algorithms are number-theoretic and algebraic structures, including groups of points of elliptic curves over finite fields.

A brief review of existing Russian-language textbooks and manuals on the mathematical foundations of cryptography is given. It is noted that the necessary components of courses on the mathematical foundations of cryptography are the elements of number theory, modular arithmetic, the theory of groups, rings and fields, the concept about construction and structure of finite fields, and in recent years also elements of the theory of elliptic curves.

The sections of the program of the course, which is read at the Belarusian State Technological University for students of the specialty “Software information security of mobile systems”, is described in detail. Particular attention is paid to the electronic educational and methodical complex (EEMC) on the subject “Mathematical foundations of cryptography”. Its structure and content are described. The examples of the pages design and the content of the electronic document are given. The methods of teaching the course “Mathematical foundations of cryptography” using EEMC and the system of individual practical tasks in the discipline are discussed.

The possibility of students' research work on this topic, the prospects for expanding the course program to reflect the latest achievements of cryptography is noted. There are discussed the possibilities of using the distance learning system for the methodical support of the course “Mathematical foundations of cryptography” which is a dynamically changing discipline currently.

Ключевые слова: математика, криптография, методика преподавания, информационные технологии, электронный учебно-методический комплекс.

Keywords: mathematics, cryptography, teaching methods, information technology, electronic educational and methodical complex.

Бурное развитие информационных технологий, их стремительное внедрение во все сферы жизни общества породило в начале XXI века огромный спрос на специалистов IT-профиля. Повсеместно возникают курсы подготовки программистов, открываются новые IT-специальности в высших учебных заведениях. Так, в 2014 году в Белорусском государственном технологическом университете (БГТУ) был организован новый факультет – факультет информационных технологий, на котором ведется обучение студентов по четырем специальностям: «Программное обеспечение информационных

технологий»; «Информационные системы и технологии»; «Дизайн электронных и веб-изданий»; «Программное обеспечение информационной безопасности мобильных систем». Программы математической подготовки студентов этих специальностей включают традиционные для технического вуза разделы с некоторым сокращением разделов непрерывной и увеличением доли дискретной математики. При этом для специальности «Программное обеспечение информационной безопасности мобильных систем» был запланирован курс «Математические основы криптографии», предусматривающий знакомство с теоретико-числовыми понятиями и алгебраическими структурами, лежащими в основе современных криптографических алгоритмов.

Изобретение в середине 70-х годов XX века концепции несимметричных криптографических систем и создание первых пригодных к практическому использованию криптографических алгоритмов этого типа произвело революционный переворот в криптографии и повлекло быструю алгебраизацию криптографии, вовлечение в криптографическую теорию и практику все новых алгебраических объектов. Как следствие, возникла проблема разработки учебных планов и программ подготовки специалистов по информационным технологиям, формирования содержания новых дисциплин и создания их качественного методического обеспечения. При этом требуется не только осветить основные понятия, используемые на практике в настоящее время, но и заложить базу для понимания новых результатов и методов в области защиты информации.

Назовем несколько учебно-методических пособий, отражающих содержание читаемых в высших учебных заведениях курсов по математическому обеспечению методов защиты информации. При этом нас в первую очередь интересуют работы, предназначенные для студентов не математических, а технических специальностей. Краткий обзор следует начать с учебного пособия [1], в котором представлен материал, необходимый для начального введения в теорию криптографических алгоритмов: теория групп, колец и полей, а также прикладная теория чисел. Заслуживает внимания также учебник [2], в котором достаточно полно и доступно изложены материалы по основным алгебраическим структурам, модулярной арифметике, полям Галуа, эллиптическим кривым, дано представление о криптосистемах, основанных на модулярной арифметике, и о квантовой криптографии. Более широкий охват материала представлен в учебнике [3], который также весьма полезен при подготовке курсов по математическим основам криптографии.

Изложение математических основ современных криптографических алгоритмов немыслимо без введения понятия группы точек эллиптической кривой над конечным полем. Применение эллиптических кривых для создания криптографических алгоритмов было независимо предложено Н. Коблицем и В. Миллером в 1985 году.

Привлекательность подхода на основе эллиптических кривых по сравнению, например, с классической системой RSA, заключается в том, что обеспечиваются те же криптографические свойства при существенно меньшей длине ключа, а следовательно, упрощается программная и аппаратная реализация криптосистем.

В настоящее время эллиптическая криптография динамично развивается и вышла на уровень использования в государственных и международных стандартах. На русском языке издана книга [4], посвященная изложению элементов теории эллиптических кривых и их применения в теоретико-числовых и криптографических алгоритмах.

Опишем учебную программу, методическое обеспечение и методику преподавания дисциплины «Математические основы криптографии» в БГТУ.

Учитывая вовлеченность в сферу современной практической криптографии таких теоретико-числовых и алгебраических структур как классы вычетов, конечные поля и группы точек эллиптических кривых, мы включили в программу дисциплины

«Математические основы криптографии» следующие основные разделы:

1. Элементы теории чисел.
2. Алгебраические структуры.
3. Поля Галуа.
4. Эллиптические кривые.

Первый раздел включает теорию делимости целых чисел, сравнения и классы вычетов, алгоритм Евклида для нахождения НОД целых чисел и решения линейных сравнений, свойства функции Эйлера, теорему Эйлера, понятие о первообразных корнях и индексах (дискретных логарифмах) в классах вычетов, применение символов Лежандра и Якоби для проверки разрешимости квадратичных сравнений. Дается представление о математических задачах факторизации целых чисел и дискретного логарифмирования, трудноразрешимость которых лежит в основе современных криптосистем с открытым ключом.

В разделе «Алгебраические структуры» рассматриваются группы, кольца, поля, дается понятие о теории делимости в кольце и о факториальных кольцах, достаточно подробно изучаются свойства кольца многочленов над полем, в частности, над конечным полем Z_p, обсуждаются понятия и свойства неприводимых многочленов, применимость алгоритма Евклида для нахождения НОД многочленов.

Третий раздел посвящен описанию полей Галуа, т.е. полей конечного порядка. Обсуждаются различные способы построения таких структур и описания их элементов, дается понятие об изоморфизме полей одного порядка, упоминаются существующие алгоритмы дискретного логарифмирования в конечных полях.

В разделе «Эллиптические кривые» описываются правила сложения элементов в группах точек эллиптических кривых над конечными полями, что иллюстрируется с помощью аналогичных кривых над полем действительных чисел. Кроме этого, обсуждается задача дискретного логарифмирования в группе точек эллиптической кривой над конечным полем.

Необходимость обеспечения курса учебно-методической литературой и отсутствие подходящих пособий, освещающих все перечисленные вопросы на доступном для студентов технических вузов уровне, привели к созданию электронного учебно-методического комплекса (ЭУМК) по дисциплине.

ЭУМК «Математические основы криптографии» представляет собой один pdf-документ, доступный студентам через систему дистанционного обучения (СДО) БГТУ [5].

Используя панель навигации, можно видеть всю структуру документа и перемещаться по его разделам (рис. 1). ЭУМК имеет четыре раздела:

– в теоретическом разделе представлены тесты лекций, содержание которых можно видеть на рис. 2;

– практический раздел объединяет материалы для проведения практических занятий и выполнения индивидуальных расчетных заданий по теории чисел и теории полей Галуа;

– раздел контроля знаний содержит материалы для текущей и итоговой аттестации, а именно примерные варианты контрольных работ и перечень теоретических вопросов для подготовки к зачету по дисциплине;

– вспомогательный раздел включает учебную программу дисциплины и список рекомендуемой для более глубокого изучения рассматриваемых вопросов курса литературы.

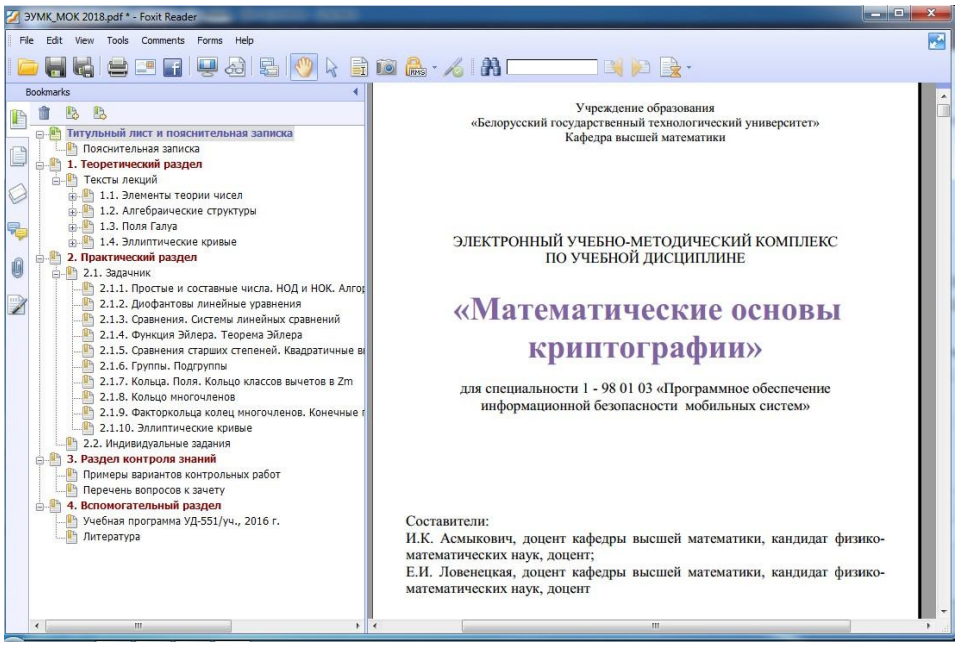

Рисунок 1. Титульный лист и структура ЭУМК
«Математические основы криптографии»

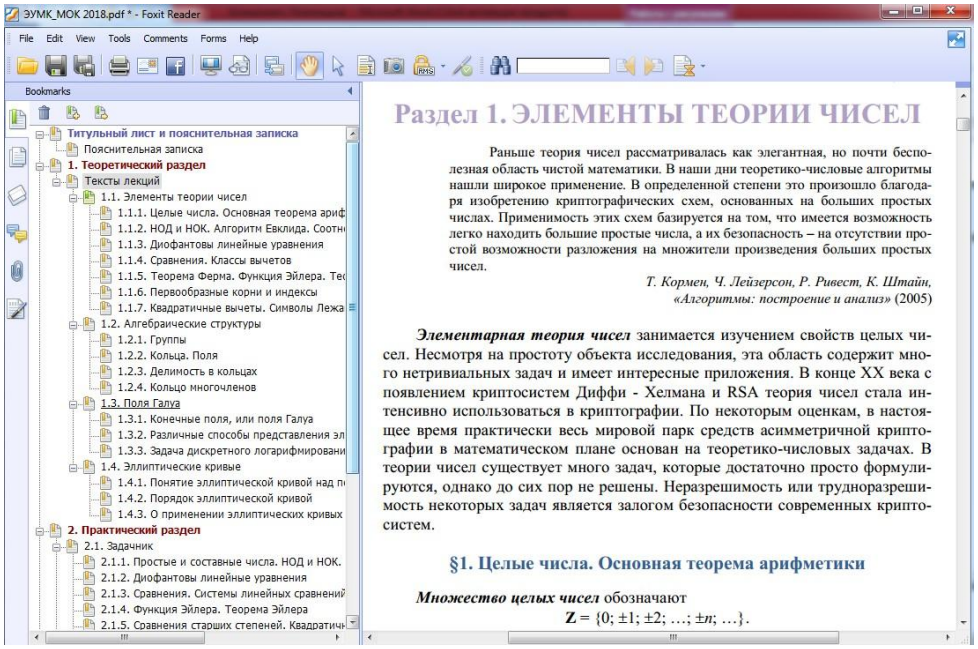

Рисунок 2. Содержание лекционного материала
в ЭУМК «Математические основы криптографии»

ЭУМК обеспечивает студентов как теоретическим материалом, позволяющим сформировать представление о месте теории чисел и основных понятий алгебры в современной криптографии и познакомиться с теорией эллиптических кривых над конечными полями как математическим обоснованием последних достижений в криптологии, так и набором заданий для проведения практических занятий и самостоятельного решения. Задачи для решения в аудитории подобраны таким образом, чтобы студенты могли освоить основные понятия курса и получить представление о свойствах и способах оперирования с изучаемыми математическими объектами. Для закрепления материала, а отчасти в силу приученности студентов IT-специальностей к

работе в режиме выполнения индивидуальных проектов, сформирован комплекс индивидуальных заданий по всем основным прикладным темам, по которым каждый студент должен отчитаться для получения зачета.

Наличие ЭУМК вносит коррективы также и в процесс чтения лекций. Появляется возможность более детального обсуждения наиболее значимых моментов и краткого упоминания остального, поскольку нет необходимости записывать подробно всю информацию.

Современная молодежь, привыкшая к постоянному использованию всевозможных гаджетов и получению ответов на любые вопросы из интернета в режиме реального времени, вообще не стремится вести полноценный конспект лекций. Однако приходится констатировать, что для незаинтересованного студента и наличие ЭУМК не способствует формированию целостного восприятия изучаемого курса. Любое методическое обеспечение и инновационные технологии преподавания эффективно работают только при условии стремления самого обучаемого к получению знаний.

При этом аналогичные технологии можно успешно использовать при организации учебно-исследовательской работы заинтересованных студентов [6]. Бурное развитие криптографических алгоритмов, использующих теоретико-числовые и алгебраические структуры, открывает хорошо успевающим студентам широкие возможности для непосредственного изучения различных существующих методов с помощью информационных технологий. Такие студенты пробуют свои силы в научно-исследовательской работе по применению методов прикладной математики и участвуют в различных конференциях и симпозиумах, начиная с младших курсов обучения в университете [7-10].

Выводы

Современный этап развития общества характеризуется широким проникновением информационно-коммуникационных технологий во все сферы жизни, что диктует необходимость и предоставляет средства для модернизации образовательного процесса высшей школы. Особую актуальность приобретают задачи оптимального отбора материала для изучения, а также воспитания у молодежи навыков логического осмысления и критического анализа поступающей информации.

Курс «Математические основы криптографии» для IT-специальностей обеспечивает знакомство студентов с теоретико-числовыми и алгебраическими структурами, вовлеченными в практику современной криптографии, а также закладывает фундамент для изучения более сложных объектов, которые могут послужить основой для построения криптографических систем в будущем. Необходимым следствием динамичного развития криптографических методов защиты информации должно быть столь же динамичное изменение программы и содержания курса по математическим основам криптографии. Так, в перспективе в программу курса, по-видимому, должны войти гиперэллиптические кривые, возможность применения которых в криптографии интенсивно исследуется в последнее время [3, 4]. Необходимость методического обеспечения столь динамично меняющегося курса весьма удачно реализуется с использованием системы дистанционного обучения [5], где имеется возможность своевременно вносить изменения в представленные материалы.

На наш взгляд, основной функцией дистанционных курсов, включаемых как часть традиционных учебных курсов, является именно предоставление студентам хорошо структурированной тщательно отобранной информации, необходимой и достаточной для изучения соответствующей дисциплины, что обеспечивает качественную основу и руководство для освоения предмета.

Литература

1. Коробейников А.Г. Математические основы криптографии: учеб. пособие. С.-Петербург: С.-Петерб. гос. ин-т точной механики и оптики (технич. ун-т), 2002. 41 с.
2. Данилова О.Ю., Думачев В.Н. Математические основы криптографии: учебник. Воронеж: Воронежский ин-т МВД России, 2017. 300 с.
3. Харин Ю.С., Агиевич С.В., Васильев Д.В., Матвеев Г.В. Криптология: учебник. Минск: БГУ, 2013. 511 с.
4. Соловьев Ю.П., Садовничий В.А., Шавгулидзе Е.Т., Белокуров В.В. Эллиптические кривые и современные алгоритмы теории чисел. Москва-Ижевск: Институт компьютерных исследований, 2003. 192 с.
5. Ловенецкая Е.И., Бочило Н.В. Первые результаты использования систем дистанционного обучения в учебном процессе кафедры высшей математики // Высшее техническое образование. Минск: БГТУ, 2018. Т. 2, №1. С. 90-94.
6. Асмыкович И.К. О применении информационных технологий для НИРС и УИРС по математике в технических университетах // Техническое творчество молодёжи. Научно-практический образовательный журнал. 2016, № 4 (98). С. 10-12.
7. Ковалевич Д.А., Лашкевич Е.М. Разделение секрета по схеме Асмута-Блума // Молодіжна наука у контексті суспільно-економічного розвитку країни: збірник тез доповідей учасників Міжнародної учнівсько-студентської інтернет-конференції, Черкаси, 5 грудня 2017 р. Черкаси: Східноєвропейський університет економіки і менеджменту, 2017. С. 211-215.
8. Хорхалёв В.В. Эллиптические кривые и их приложения в криптографии // 68-я научно-техническая конференция учащихся, студентов и магистрантов: сб. науч. работ: в 4-х ч. – Минск: БГТУ, 2017. – Ч. 4. С. 278-281.
9. Марчук К.С. Применение китайской теоремы об остатках в алгоритме RSA // 69-я научно-техническая конференция учащихся, студентов и магистрантов: сб. науч. работ: в 4-х ч. – Минск: БГТУ, 2018. – Ч. 4. С. 283-286.
10. Чернявский А.Л. Задача Штейнера // 69-я научно-техническая конференция учащихся, студентов и магистрантов: сб. науч. работ: в 4-х ч. – Минск: БГТУ, 2018. – Ч. 4. С. 279-283.