Scientific journal
PHYSICAL AND MATHEMATICAL EDUCATION
Has been issued since 2013.

Науковий журнал
ФІЗИКО-МАТЕМАТИЧНА ОСВІТА
Видається з 2013.

ISSN 2413-158X (online)
ISSN 2413-1571 (print)

http://fmo-journal.fizmatsspu.sumy.ua/

Асмыкович И.К., Ловенецкая Е.И. О методическом обеспечении курса «Математические основы криптографии» в белорусском государственном технологическом университете. Фізико-математична освіта. 2019. Випуск 1(19). С. 18-23.

Asmykovich I.K., Lovenetskaya E.I. About The Methodical Support Of The "Mathematical Foundations Of Cryptography" Course In Belarusian State Technological University. Physical and Mathematical Education. 2019. Issue 1(19). P. 18-23.

DOI 10.31110/2413-1571-2019-019-1-003
УДК 378.147:512.5

И.К. Асмыкович
Белорусский государственный технологический университет, Беларусь
asmik@tut.by
Е.И. Ловенецкая
Белорусский государственный технологический университет, Беларусь
ei_blinova@mail.ru

О МЕТОДИЧЕСКОМ ОБЕСПЕЧЕНИИ КУРСА «МАТЕМАТИЧЕСКИЕ ОСНОВЫ КРИПТОГРАФИИ» В БЕЛОРУССКОМ ГОСУДАРСТВЕННОМ ТЕХНОЛОГИЧЕСКОМ УНИВЕРСИТЕТЕ

АННОТАЦИЯ

Формулировка проблемы. *Статья посвящена анализу содержания и методического обеспечения курса «Математические основы криптографии» для студентов IT-специальностей.*

Материалы, методы. *Анализ доступных интернет-ресурсов и учебно-методических материалов с целью обобщения опыта преподавания теоретико-числовых и алгебраических основ современной криптографии, осуществлено теоретическое проектирование и моделирование учебного процесса с целью формирования у студентов современных знаний и практических навыков по математическим основам методов защиты информации*

Результаты. *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 курса «Математические основы криптографии» с использованием ЭУМК и системы индивидуальных практических заданий по дисциплине.*

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.

Выводы. *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».*

КЛЮЧЕВЫЕ СЛОВА: *математика, криптография, методика преподавания, информационные технологии, электронный учебно-методический комплекс.*

ВВЕДЕНИЕ

Постановка проблемы. 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, в основном, традиционные для технического вуза разделы, однако

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 фактически произвело революционный переворот в криптографии и позволило решать элегантным и достаточно простым способом сложнейшие задачи идентификации, аутентификации, управления ключами и ряд других. Одновременно это повлекло быструю алгебраизацию криптографии, вовлечение в криптографическую теорию и практику все новых алгебраических объектов.

Как следствие, возникла проблема адекватного реагирования учебных планов и программ подготовки IT-специалистов, формирования содержания дисциплин и создания их качественного методического обеспечения, позволяющего 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.

Анализ актуальных исследований. Анализ имеющейся литературы и доступных интернет-источников показал, что в большинстве высших учебных заведений, готовящих специалистов IT-профиля, в программы обучения студентов включаются в том или ином виде курсы защиты информации и криптографии, ведется активная работа по созданию учебных пособий, посвященных тем или иным аспектам математических основ криптографии.

Назовем несколько учебно-методических пособий, отражающих содержание читаемых в высших учебных заведениях курсов. При этом нас в первую очередь интересуют работы, предназначенные для студентов не математических, а технических специальностей.

Краткий обзор следует начать с учебного пособия (Коробейников, 2002), в которой представлен материал, необходимый для начального введения в теорию криптографических алгоритмов: теория групп, колец и полей, а также прикладная теория чисел. В пособии (Галуев, 2003) рассмотрены вопросы стойкости криптографических систем и алгоритмов, элементы теории чисел и теории конечных полей, обсуждаются понятия односторонней функции и хэш-функции, дана общая характеристика различных типов шифров и классов криптосистем, приведены алгоритмы Диффи-Хеллмана, RSA, Эль Гамаля. Достаточно краткое, но полное и строгое изложение алгебраических основ теории и практики обработки дискретных сигналов и защиты информации, включая описание теории полей Галуа, приведено в (Липницкий, 2006). В пособии (Онацкий & Йона, 2010) рассмотрены методы шифрования с открытыми ключами, цифровой подписи, основные криптографические протоколы и хэш-функции, криптосистемы на эллиптических кривых, подробно описаны алгоритмы, лежащие в основе международных стандартов, подчеркивается необходимость знания понятий и результатов теории чисел для понимания криптографических алгоритмов. Заслуживает внимания также учебник (Данилова & Думачев, 2017), 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 учебниках (Нестеренко, 2012) и (Харин и др., 2013), которые также весьма полезны при подготовке курсов по математическим основам криптографии. Описание большого количества теоретико-числовых алгоритмов с обоснованием их корректности и оценками трудоемкости можно найти в монографии (Василенко, 2003) и более доступных для понимания книгах (Черемушкин, 2002) и (Ишмухаметов, 2011). Актуальным вопросам алгоритмической теории чисел посвящена также прекрасно написанная книга американских математиков Р. Крэндалла и К. Померанса (Крэндалл & Померанс, 2011).

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 изданы книги (Болотов и др., 2006) и (Соловьев и др., 2003), посвященные изложению элементов теории эллиптических кривых и их применения в теоретико-числовых и криптографических алгоритмах. Отметим, что в книгах (Василенко, 2003), (Ишмухаметов, 2011), (Крэндалл & Померанс, 2011), (Харин и др., 2013) также уделяется внимание вопросам использования эллиптических кривых в криптографических алгоритмах.

Таков краткий перечень наиболее доступных источников, который может быть использован для построения курса по теоретико-числовым и алгебраическим основам криптографии в техническом вузе.

Цель статьи – описание учебной программы, методического обеспечения и методики преподавания дисциплины «Математические основы криптографии» в БГТУ.

МЕТОДЫ ИССЛЕДОВАНИЯ

Проведен анализ доступных интернет-ресурсов и учебно-методических материалов с целью обобщения опыта преподавания теоретико-числовых и алгебраических основ современной криптографии, осуществлено теоретическое проектирование и моделирование учебного процесса с целью формирования у студентов современных знаний и практических навыков по математическим основам методов защиты информации.

РЕЗУЛЬТАТЫ ИССЛЕДОВАНИЯ

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:

Элементы теории чисел.

Алгебраические структуры.

Поля Галуа.

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. 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.

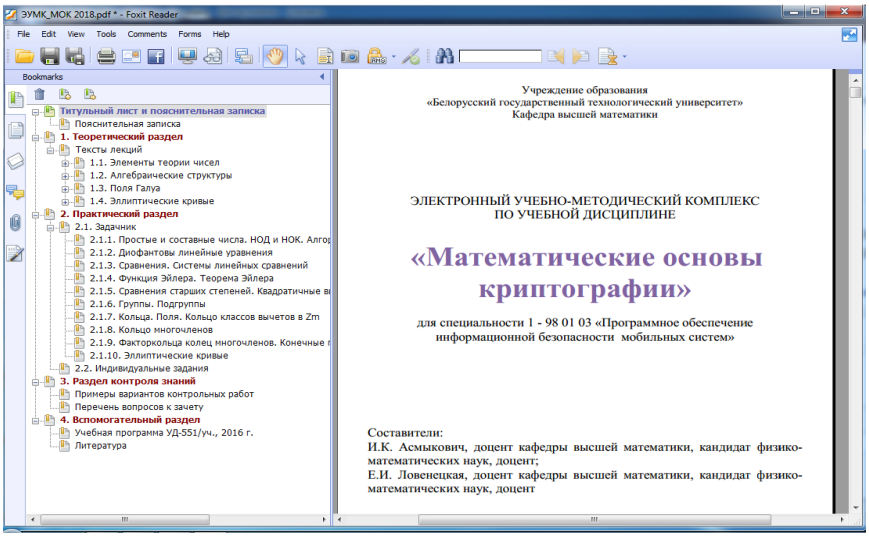

Рис. 1. Титульный лист и структура ЭУМК «Математические основы криптографии»

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.

ОБСУЖДЕНИЕ

Бурное развитие криптографических алгоритмов, использующих теоретико-числовые и алгебраические структуры, открывает заинтересованным студентам широкие возможности для изучения различных существующих методов и пробы

своих сил в научно-исследовательской работе (см., например, (Ковалевич & Лашкевич, 2017; Хорхалев, 2017)).

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.

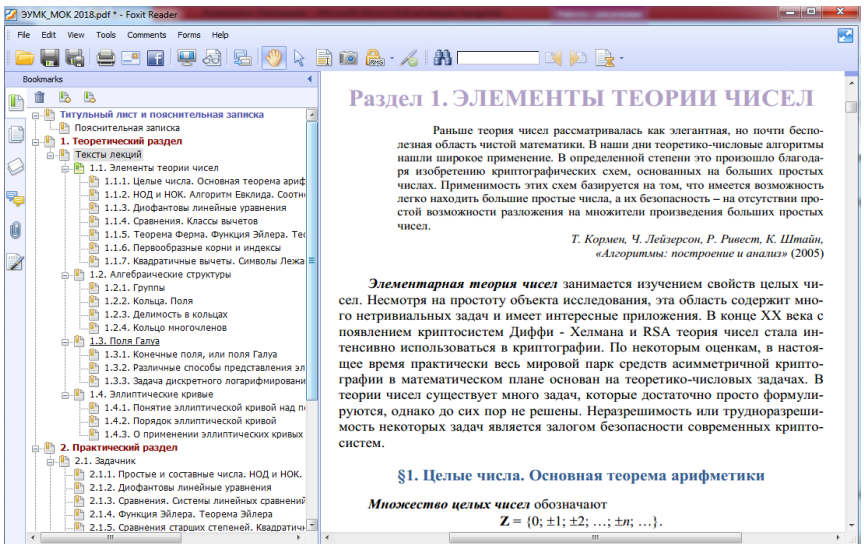

Рис. 2. Содержание лекционного материала в ЭУМК «Математические основы криптографии»

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 работе с хорошими студентами по применению различных разделов математики (Асмыкович, 2018).

ВЫВОДЫ ПЕРСПЕКТИВЫ ДАЛЬНЕЙШИХ ИССЛЕДОВАНИЙ

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 (см. (Болотов и др., 2006), (Соловьев и др., 2003)).

Необходимость методического обеспечения столь динамично меняющегося курса весьма удачно реализуется с использованием системы дистанционного обучения (Ловенецкая & Бочило, 2018), 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.

Список использованных источников

1. Асмыкович И.К. Опыт организации работы по применению математики студентами технического университета. *Научная деятельность как путь формирования профессиональных компетентностей будущего специалиста (НПК-2018) : материалы Межд. научно-практической конф., 6-7 декабря 2018 г., г. Сумы*. В 2 ч. Ч.2. Сумы: ФЛП Цёма С.П., 2018. С. 110-111.
2. Болотов А.А., Гашков С.Б., Фролов А.Б., Часовских А.А. *Элементарное введение в эллиптическую криптографию: Алгебраические и алгоритмические основы*. Москва: КомКнига, 2006. 328 с.
3. Василенко О.Н. *Теоретико-числовые алгоритмы в криптографии*. Москва: МЦНМО, 2003. 328 с.
4. Галуев Г.А. *Математические основы криптологии*: учебно-метод. пособие. Таганрог: Изд-во ТРТУ, 2003. 120 с.
5. Данилова О. Ю., Думачев В.Н. *Математические основы криптографии*: учебник. Воронеж: Воронежский ин-т МВД России, 2017. 300 с.

6. Ишмухаметов Ш.Т. *Методы факторизации натуральных чисел*: учеб. пособие. Казань: Казан. ун-т, 2011. 190 с.
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. 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.
9. Крэндалл Р., Померанс К. *Простые числа: Криптографические и вычислительные аспекты*. Пер. с англ. / Под ред. и с предисл. В. Н. Чубарикова. Москва: УРСС: Книжный дом «ЛИБРОКОМ», 2011. 664 с.
10. Липницкий В. А. *Современная прикладная алгебра. Математические основы защиты информации от помех и несанкционированного доступа*: учеб.-метод. пособие по курсу «Высшая математика» для студ. спец. «Сети телекоммуникаций» и «Информатика» всех форм обуч. 2-е изд., испр. Минск: БГУИР, 2006. 88 с.
11. 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.
12. Нестеренко А.Ю. *Теоретико-числовые методы в криптографии*: учеб пособие. Москва: Моск. гос. ин-т электроники и математики, 2012. 224 с.
13. Онацкий А.В., Йона Л.Г. *Асимметричные методы шифрования. – Модуль 2. Криптографические методы защиты информации в телекоммуникационных системах и сетях*: учеб. пособие / Под ред. Н.В. Захарченко. Одесса: ОНАС им. А.С. Попова, 2010. 148 с.
14. 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.
15. Харин Ю.С., Агиевич С.В., Васильев Д.В., Матвеев Г.В. *Криптология*: учебник. Минск: БГУ, 2013. 511 с.
16. Хорхалёв В.В. Эллиптические кривые и их приложения в криптографии. *68-я научно-техническая конференция учащихся, студентов и магистрантов, 17-22 апреля, Минск: сб. научных работ.* В 4 ч. Ч. 4. Минск: БГТУ, 2017. С. 278-281.
17. Черемушкин А.В. *Лекции по арифметическим алгоритмам в криптографии*. Москва: МЦНМО, 2002. 104 с.

References

1. Asmykovich, I.K. (2018). Opyt organizatsii raboty po primeneniyu matematiki studentami tekhnicheskogo universiteta [Experience in the organization of work on the application of mathematics by students of a technical university]. Proceedings of the International scientific and practical Conference *«Nauchnaja dejatel'nost' kak put' formirovanija professional'nyh kompetentnostej budushhego specialista (NPK-2018)» - «Scientific activity as a way of forming the professional competencies of a future specialist (NPC-2018)»*, 6-7 dekabrja 2018 g., Sumy (part 2, pp. 110-111). Sumy: FLP Cjoma S.P. [in Russian].
2. Bolotov, A.A., Gashkov, S.B., Frolov, A.B. & Chasovskikh, A.A. (2006). *Elementarnoye vvedeniye v ellipticheskuyu kriptografiyu: Algebraicheskiye i algoritmicheskiye osnovy [An elementary introduction to elliptical cryptography: Algebraic and algorithmic foundations]*. Moskva: KomKniga [in Russian].
3. Vasilenko, O.N. (2003). *Teoretiko-chislovyye algoritmy v kriptografii [Number-theoretic algorithms in cryptography]*. Moskva: MCNMO [in Russian].
4. Galuyev, G.A. (2003). *Matematicheskiye osnovy kriptologii [Mathematical foundations of cryptology]:* uchebno-metod. posobiye. Taganrog: Izd-vo TRTU [in Russian].
5. 5.Danilova, O.Yu. & Dumachev, V.N. (2017). *Matematicheskiye osnovy kriptografii [Mathematical foundations of cryptography]:* uchebnik. Voronezh: Voronezhskij in-t MVD Rossii [in Russian].
6. Ishmuhametov, Sh.T. (2011). *Metody faktorizacii natural'nyh chisel [Methods of factoring natural numbers]*: ucheb. posobie. Kazan': Kazan. un-t [in Russian].
7. Kovalevych, D.A. & Lashkevych, E.M. (2017). Razdelenye sekreta po skheme Asmuta-Bluma [Separation of the secret according to the Asmuta-Bloom scheme]. Abstracts of Papers of the International Student-Student Internet Conference *«Molodizhna nauka u konteksti suspilno-ekonomichnoho rozvytku krainy» - «Youth Science in the Context of Socio-Economic Development of the Country»:* zbirnyk tez dopovidei uchasnykiv Mizhnarodnoi uchnivsko-studentskoi internet-konferentsii, Cherkasi, 5 grudnja 2017. (pp. 211-215). Cherkasi: Shidnoevropejs'kij universitet ekonomiki i menedzhmentu [in Russian].
8. Korobeynikov, A.G. (2002). *Matematicheskiye osnovy kriptografii [Mathematical foundations of cryptography]*: ucheb. posobiye. S.-Peterburg: C.-Peterb. gos. in-t tochnoy mekhaniki i optiki (tekhnich. un-t) [in Russian].
9. Krjendall, R. & Pomerans, K. (2011). *Prostye chisla: Kriptograficheskie i vychislitel'nye aspekty [Prime numbers: Cryptographic and computational aspects]*. Trans. from English. / Ed. V. N. Chubarikov. Moskva: URSS: Knizhnyj dom «LIBROKOM» [in Russian].
10. Lipnitskiy, V. A. (2006). *Sovremennaya prikladnaya algebra. Matematicheskiye osnovy zashchity informatsii ot pomekh i nesanktsionirovannogo dostupa [Modern applied algebra. Mathematical foundations of information protection from interference and unauthorized access]:* ucheb.-metod. posobiye po kursu «Vysshaya matematika» dlya stud. spets. «Seti telekommunikatsiy» i «Informatika» vseh form obuch. 2nd ed., corr. Minsk: BGUIR [in Russian].
11. Lovenetskaya, E.I. & Bochilo, N.V. (2018). Pervyye rezul'taty ispol'zovaniya sistem distantsionnogo obucheniya v uchebnom protsesse kafedry vysshey matematiki [First Results of Using Distance Learning Systems in the Educational Process of the Department of Higher Mathematics]. *Vysshee tehnicheskoe obrazovanie - Higher Technical Education*. Vol. 2, 1, 90-94 [in Russian].
12. Nesterenko, A.Yu. (2012). *Teoretiko-chislovyye metody v kriptografii [Number theory methods in cryptography]*: ucheb. posobiye. Moskva: Mosk. gos. in-t jelektroniki i matematiki [in Russian].
13. Onatskiy, A.V. & Yona, L.G. (2010). *Asimmetrichnyye metody shifrovaniya. – Modul' 2. Kriptograficheskiye metody zashchity informatsii v telekommunikatsionnykh sistemakh i setyakh [Asymmetric encryption methods. - Module 2. Cryptographic*

methods for protecting information in telecommunication systems and networks]: ucheb. posobiye / Ed. N.V. Zakharchenko. Odessa: ONAS im. A.S. Popova [in Russian].

14. Solov'yev, Yu.P., Sadovnichiy, V.A., Shavgulidze, E.T. & Belokurov, V.V. (2003). *Ellipticheskiye krivyye i sovremennyye algoritmy teorii chise [Elliptic curves and modern number theory algorithms].* Moskva-Izhevsk: Institut komp'juternyh issledovanij [in Russian].
15. Harin, Yu.S., Agiyevich, S.V., Vasil'yev, D.V. & Matveyev, G.V. (2013). *Kriptologiya [Cryptology]:* uchebnik. Minsk: BGU [in Russian].
16. Horhaljov, V.V. (2017). Jellipticheskie krivye i ih prilozhenija v kriptografii [Elliptic curves and their applications in cryptography]. Proceedings of the Conference *«68-ja nauchno-tehnicheskaja konferencija uchashhihsja, studentov i magistrantov» - «The 68th Scientific and Technical Conference of Pupils, Students and Undergraduates»,* 17-22 aprelja, Minsk (part 4, pp.278-281). Minsk: BGTU [in Russian].
17. Cheremushkin, A.V. (2002). *Lekcii po arifmeticheskim algoritmam v kriptografii [Lectures on arithmetic algorithms in cryptography]*. Moskva: MCNMO [in Russian].

ABOUT THE METHODICAL SUPPORT OF THE "MATHEMATICAL FOUNDATIONS OF CRYPTOGRAPHY" COURSE IN BELARUSIAN STATE TECHNOLOGICAL UNIVERSITY

I.K. Asmykovich, E.I. Lovenetskaya

Belarusian State Technological University, Belarus

Abstract.

Formulation of the problem. *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.*

Materials, methods. *Analysis of available online resources and teaching materials for the purpose of generalizing the experience of teaching the theoretical numerical and algebraic foundations of modern cryptography; theoretical designing and modeling of the educational process with the purpose of formation of modern knowledge and practical skills on the mathematical bases of methods of information protection was carried out.*

Results. *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.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.*

Conclusions. *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.*

Key words: *mathematics, cryptography, teaching methods, information technology, electronic educational and methodical complex.*