УДК 510

В.Г. Дурнев

Россия, Ярославль, Ярославский государственный университет
имени П.Г. Демидова

ОБ ОПЫТЕ «УСИЛЕНИЯ» НЕКОТОРЫХ МАТЕМАТИЧЕСКИХ ДИСЦИПЛИН УЧЕБНОГО ПЛАНА ПО СПЕЦИАЛЬНОСТИ «КОМПЬЮТЕРНАЯ БЕЗОПАСНОСТЬ»

Приводятся некоторые сведения об опыте математического подкрепления за счет вузовского компонента таких дисциплин, как «Алгебра», «Математическая логика и теория алгоритмов», «Теоретико-числовые методы в криптографии», «Криптографические методы защиты информации», «Модели безопасности компьютерных систем», «Методы алгебраической геометрии в криптографии» и «Математический анализ».

Ключевые слова: теория чисел; теоретико-числовые методы в криптографии; теория алгоритмов; алгоритмически неразрешимые проблемы; сложность выполнения алгоритма; криптография на эллиптических кривых; конечные поля и неприводимые над ними полиномы в алгоритмах шифрования.

«Государственный образовательный стандарт высшего профессионального образования. Специальность 075200 «Компьютерная безопасность» (Москва, 2000), подпункт 6.1.2 пункта 6.1 «Требования к разработке основной образовательной программы подготовки математика» раздела 6. «Требования к разработке и условиям реализации основной образовательной программы подготовки выпускника по специальности 075200-Компьютерная безопасность» гласит: «При реализации основной образовательной программы высшее учебное заведение имеет право: ... в каждом блоке дисциплин использовать часы национально-регионального (вузовского) компонента для образования новых дисциплин этого блока и/или усиления дисциплин федерального компонента». На математическом факультете Ярославского государственного университета имени П.Г. Демидова еще в 2000 году при разработке Учебного плана по специальности «Компьютерная безопасность» пошли по пути использования часов национально-регионального (вузовского) компонента для усиления дисциплин федерального компонента путем введения новых дисциплин, поддерживающих и усиливающих дисциплины федерального компонента.

Дисциплина «Введение в теорию множеств и логическую символику» предназначена для студентов первого курса (1-ый семестр, 3 часа в неделю). Она подводит теоретико-множественный фундамент под математические дисциплины – через понятие «множество» определяются такие математические понятия, как «упорядоченная пара и упорядоченный набор элементов», «соответствие», «отношение», «отображение» и «функция», т.е. строится теоретико-множественный «фундамент» математики. С использованием понятий «отношение эквивалентности», «класс эквивалентности» и «фактормножество по отношению эквивалентности» строится цепочка расширений числовых систем: «система натуральные числа» (система Пеано) - «кольцо целых чисел» - «поле рациональных чисел» - «поле действительных чисел» - «поле комплексных чисел» - «алгебра кватернионов». На основе понятий «инъективное отображение» и «биективное отображение» определяется понятие «равномощности множеств», «мощность множества А не превосходит мощность множества В». Доказывается теорема Г.Кантора о мощности множества подмножеств данного множества, изучаются счетные и континуальные множества. Весь этот материал в дальнейшем используется при изучении таких математических дисциплин, как «Математический анализ», «Алгебра» и «Теория вероятностей», а так же дисциплин специализации. Изучается некоторый начальный материал по математической логике – логика высказываний и исчисление высказываний. Очень кратно обсуждается логика предикатов. Все это более подробно будет изучаться в дисциплине «Математическая логика и теория алгоритмов», а на этом этапе – лишь первоначальное знакомство с базовыми понятиями теории множеств и математической логики.

Дисциплина «Алгебра» усиливается целым рядом дисциплин. Это, прежде всего, «Линейная алгебра» (второй курс, 3-4 семестры, 4 часа в неделю), в которой изучается традиционный материал: векторные пространства, линейные отображения, билинейные и квадратичные формы, полилинейные отображения. Подробно изучаются линейные операторы и жорданова нормальная форма. В евклидовом и эрмитовом пространствах изучаются сопряженные операторы и доказывается спектральная теорема для нормальных операторов. Завершается курс изучением аффинных и евклидовых точечных пространств, выпуклых множеств, задачи линейного программирования, подходов к ее решению Левина-Хачияна, квадрик и их канонических уравнений. Дисциплина «Избранные вопросы алгебры» (второй курс, 2-ой семестр, 3 часа в неделю) посвящена изучению элементов теории полей – конечные и алгебраические расширения, «теоремы о башне полей» и линейных рекуррентных последова-

тельностей». Дисциплина «Общая алгебра», другое название - «Фундаментальные алгебраические структуры» посвящена изучению «87нновских» алгебраических структур – группоидов, полугрупп, моноидов, групп, колец и полей. При изучении групп особое внимание уделяется комбинаторной теории групп, нашедшей применение в современной криптографии (« Group-based cryptography») – заданию групп образующими и определяющими соотношениями, фундаментальным проблемам М.Дэна, теоремам П.С. Новикова и С.И. Адяна – М. Рабина об алгоритмической неразрешимости соответствующих проблем. Методами комбинаторной теории групп доказывается классическая теорема о строении конечно порожденных абелевых групп. Обсуждаются теоретико-групповые аспекты некоторых криптоалгоритмов, лежащих в основе современных стандартов шифрования, цифровой подписи и выработки хэш-значения. Изучаются ассоциативные кольца и кольцевые конструкции, идеалы, факторкольца, теоремы о гомоморфизмах для колец. Особое внимание уделяется теории полей и их расширений – конечных и алгебраических, изучению конечных полей и их мультипликативных групп, неприводимых и примитивных полиномов над конечными полями. Достаточно спорным является материал, посвященный модулям и представлениям групп и алгебр. Завершается курс углубленным изучением линейных рекуррентных последовательностей и систем линейных уравнений над кольцом целых чисел, что позволяет подвести слушателей к пониманию важности вопроса о сложности алгоритма, решающего данную задачу, наряду с вопросом о существовании самого алгоритма. Дисциплина «Общая алгебра» служит «фундаментом» и для дисциплины «Методы алгебраической геометрии в криптографии».

Дисциплина «Математическая логика и теория алгоритмов» «развивается и усиливается» такими дисциплинами, как «Теория алгоритмов» (четвертый курс, 7-ой семестр, 3 часа в неделю), «Сложность вычислений» (четвертый курс, 8-ой семестр, 3 часа в неделю), «Алгебраическая алгоритмика» (2-3 курсы, 4-ый и 5-ый семестры, 3 часа в неделю) и «Теория автоматов» (5-ый курс, 10-ый семестр, 3 часа в неделю). Дисциплина «Теория алгоритмов» посвящена двум подходам к уточнению интуитивного понятия «алгоритм» - в терминах частично рекурсивных функций и через понятие машины Тьюринга, доказывается «эквивалентность» этих двух подходов – функция вычислима по Тьюрингу тогда и только тогда, когда она частично рекурсивна. В ходе доказательства слушатели знакомятся с «фундаментальным математическим понятием» - понятием «арифметизации теории», что представляется чрезвычайно важным само по себе. «Вершиной» теории служит теорема Райса об алгорит-

мической нераспознаваемости свойств вычислимых функций по «их программам», что чрезвычайно важно для будущих специалистов в области компьютерных наук. Обсуждаются алгоритмически неразрешимые проблемы из различных разделов математики – теории алгоритмов, математической 88нновки, алгебры, теории чисел, теории формальных грамматик, теории обыкновенных дифференциальных уравнений, топологии, математического анализа, теории конечных автоматов, что позволяет подвести слушателей к пониманию утверждения о том, что «алгоритмически неразрешимые проблемы проникли во все разделы математики» и с этим надо считаться, как с объективной реальностью. Алгоритмическая неразрешимость проблемы остановки для машин Тьюринга используется в дисциплине «Модели безопасности компьютерных систем» при изучении модели HRU дискреционного управления доступом. Из-за недостатка времени обычно не удается обсудить другие вычислительные модели – нормальные алгорифмы А.А.Маркова, машины с произвольным доступом к памяти и диофантовы множества и функции (10-ая проблема Д.Гильберта), хотя это и планируется сделать за счет некоторого перераспределения материала и часов. В дисциплине «Сложность вычислений» основное внимание уделяется вопросу о сложности распознавания языков на многоленточных детерминированных и недетерминированных машинах Тьюринга. При этом основное внимание по ряду причин уделяется обсуждению классов P-TIME и NP-TIME, NP-трудных и NP-полных проблем, что представляется достаточно близким интересам современной теоретической информатики (Computer Science) и асимметрической криптографии (Public Key Cryptography). Слушатели знакомятся с некоторыми подходами к сложностной классификации языков и проблем. К этому же блоку относится и дисциплина «Алгебраическая алгоритмика», в которой изучаются прежде всего конкретные алгоритмы для кольца целых чисел и колец многочленов над полями и кольцами, вычисления в конечных полях, дискретное преобразование Фурье (ДПФ) и быстрое преобразование Фурье (БПФ). Дисциплина «Алгоритмы на графах» так же посвящена изучению конкретных алгоритмов.

Дисциплина «Теория чисел» (второй курс, 3-ий семестр, 2 часа в неделю) служит основой для дисциплины «Теоретико-числовые методы в криптографии». В ней изучаются вопросы, связанные с натуральными и целыми числами: теория делимости, сравнения и вычеты, квадратичные вычеты, закон взаимности, теоремы Ферма и Эйлера, играющие важную роль в системе RSA, теоретико-числовые функции, цепные дроби, простые числа и закон их распределения, распределение простых чисел в арифметических прогрессиях

(теорема Дирихле), первообразные корни и индексы, что, как известно, очень важно для современной асимметричной криптографии. Эти знания используются и при изучении некоторых разделов дисциплины «Криптографические методы защиты информации».

Знания, полученные слушателями при изучении дисциплин «Теория графов» и «Алгоритмы на графах», облегчают им изучение, в частности, модели Take-Grant в дисциплине «Модели безопасности компьютерных систем».

Дисциплины «Теория автоматов» и «Комбинаторика» служат дополнением к дисциплине «Дискретная математика».

Дисциплина «Топология» дополняет дисциплину «Математический 89ннолиз», в частности, через изучение общего понятия «непрерывность» в 89нновацческих и топологических пространствах.

Дисциплина «История математики» вносит вклад в общематематическую культуру выпускников.