А.Е.ЖУКОВ

О МАТЕМАТИЧЕСКОЙ ПОДГОТОВКЕ СПЕЦИАЛИСТОВ В ОБЛАСТИ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

В начале приведем несколько цитат о современном математическом образовании, взятых из статьи академика В.И. Арнольда [*)] «Антинаучная революция и математика», опубликованной в Вестнике Российской Академии Наук, том 69, № 6, с. 553-558, 1999 г.

«Расцвет математики в уходящем столетии сменяется тенденцией подавления науки и научного образования обществом и правительствами большинства стран мира. … Правительства всех стран начали исключать математические науки из программ средней школы. … Французское министерство образования, науки и технологии предполагает втрое сократить школьные учебники математики».

«Руководство биологического факультета университета в Геттингене обратилось к математикам с просьбой прочесть студентам курс теории чисел. Математики, сперва озадаченные этим предложением, обнаружили, что под теорией чисел биологи понимали сложение простых дробей. Многие геттингенские студенты предпочитают складывать числители с числителями и знаменатели со знаменателями, подобно американским студентам: 1/3+ 1/2 = 2/5».

«До сих пор уничтожение культуры, науки и образования (в частности, математики и математического образования) в России идет медленнее, чем в более цивилизованных странах. … К сожалению, сейчас уровень математической грамотности страны в целом начал катастрофически падать. Запланированная Министерством образования "гуманизация" и "гуманитаризация" предусматривает существенное уменьшение числа часов на математику с использованием высвободившихся часов на такие предметы, как макраме и коневодство. … Видимо, таким способом стремятся приблизить наш (достаточно высокий) уровень математического образования к американскому (традиционно низкому) в то самое время, когда сами американцы начинают перенимать наш опыт для радикального улучшения своего математического образования, которое они поставили себе целью сделать лучшим в мире».

Приведенные выше цитаты относятся, в основном, к школьному образованию, однако каждый, связанный с преподаванием в высшей школе, может засвидетельствовать их справедливость. Несмотря на существенно ухудшившийся уровень школьного математического образования, в технических вузах также прослеживается тенденция к сокращению дисциплин, имеющих непосредственное отношение к будущей профессиональной деятельности учащегося. Учащиеся бессмысленно нагружаются огромным количеством легковесных дисциплин типа валеологии, информациологии, основ менеджмента и маркетинга, организации производства и т.д. В глазах руководства все это выглядит очень современным и прогрессивным: учащиеся приобщаются «общечеловеческим ценностям», постигают основы рыночной экономики. Хотя очевидно, что с точки зрения той же рыночной экономики гораздо важнее, чтобы молодой специалист обладал глубокими узкопрофессиональными знаниями, а не нахватался слов и понятий из экономического или менеджерского лексикона. Тем более что весьма проблематично то, что молодой выпускник технического вуза по специальности, скажем, программист или системный администратор (хотя многие современные начальники спутают его с администратором магазина) станет заниматься маркетингом или организацией производства. Если он этим и займется – то по прошествии некоторого времени и после определенного карьерного роста. Но в этом случае ему будут полезнее не те поверхностные и отрывочные сведения, которые он получает в своем техническом вузе,

---

[*)] Арнольд Владимир Игоревич – академик, главный научный сотрудник Математического института им. В.А. Стеклова РАН

а углубленные специализированные курсы, которые он выберет сам или на которые будет направлен своим руководством. А в итоге всего – студент недополучает образование по своей основной специальности, не приобретя ничего существенного взамен.

Мне трудно сказать, что является источником этих тенденций – желание ли руководства министерства образования в купе с руководством вузов продемонстрировать мировому сообществу свою прогрессивность, лоббирование своих интересов многочисленными коллективами бывших кафедр Истории КПСС, Политэкономии, Научного коммунизма и др. или что-либо другое. Однако, указанные тенденции имеют место и отмечаются, как видно из приведенных выше цитат, не только мною.

Другая сторона проблемы касается самой направленности математического образования в рамках специальности «Информационная безопасность». Фундаментальная подготовка для специалистов по информатике и, в частности, защите информации должна отображать специфику этих специальностей, что, прежде всего, связано с формированием базовых знаний по информатике и математическим дисциплинам, что в свою очередь обуславливает требования, предъявляемые к содержанию читаемых в вузе теоретических курсов по информатике и высшей математике. Однако, формирование у специалистов базовых знаний по математике до сих пор происходит по стандартным программам, включающим в себя в основном традиционные математические дисциплины, такие, как математический анализ, аналитическая геометрия, линейная алгебра, дифференциальные уравнения, уравнения математической физики, операционное исчисление, теория вероятностей и математическая статистика. Действительно, на протяжении десятков, если не сотен лет любому техническому специалисту (и инженеру-строителю и конструктору космической техники), как правило, вполне хватало математической подготовки, полученной в рамках указанных дисциплин. Положение кардинальным образом меняется, если рассматривать профессиональную деятельность специалиста в области зашиты информации. Для работы в этой области традиционной “высшей математики для технических вузов” будет катастрофически не хватать, более того, бóльшая часть изученных в вузе математических дисциплин оказывается бесполезной для описания и моделирования информационных процессов. Те же разделы математики, которые должны для этого использоваться, по инерции считаются “абстрактными”, “чисто математическими” дисциплинами и изучаются на математических факультетах университетов, да и то зачастую не как обязательные курсы, а спецкурсы по выбору.

На рис.1 приведена схема, изображающая основные математические дисциплины, используемые в работе специалиста по информационной безопасности, а так же отражены связи между этими математическими дисциплинами. Так, например, из схемы видно, что для изучения алгебраической теории кодирования необходимо предварительное знакомство с линейной алгеброй, высшей алгеброй (точнее с алгебраическими системами – группами, кольцами, полями) и некоторыми вопросами комбинаторики.

Во всем мире уже давно преподается сформировавшийся несколько десятилетий тому назад комплекс дисциплин, называющийся, как правило, «Theoretical Foundations of Computer Science» и охватывающий большинство дисциплин, приведенных на указанной схеме. В нашей же стране, как правило, изучение этих дисциплин ограничивается куцым курсом «Дискретная математика» в течение которого в лучшем случае удается дать поверхностное представление о некоторых из указанных дисциплин, в то время как от грамотного специалиста требуется умение самостоятельно строить адекватные математические модели информационных процессов, что подразумевает совсем другой уровень владения математическим аппаратом.

Специалистам (но, к сожалению, не руководителям вузов) давно стала понятна негодность существующего положения вещей. Инженерные кафедры выходят из этого положения с помощью самодеятельности: необходимые разделы математики читаются самими инженерами в рамках тех или иных инженерных курсов. Однако, такой выход из положения тоже не может быть признан удовлетворительным. В качестве аргумента я

обычно привожу следующую фразу: «Все мы более или менее свободно ВЛАДЕЕМ русским языком. Однако, многие ли из нас, не имея специального образования, осмелятся УЧИТЬ русскому языку». А ведь математика – язык не менее трудный, чем русский.

В настоящее время на кафедре «Информационная безопасность» МГТУ им. Баумана необходимый минимум математических дисциплин, образующих теоретический базис информационной безопасности, читается в различных курсах, разбросанных по 1, 2, 5, 7, 8 семестрам, причем частично – под другими названиями (например, под названием «Информатика» на 1-2 семестрах), частично – факультативно (как «Комбинаторика» на 5 семестре, не включенная в учебный план и не обеспеченная аудиториями). Насколько мне известно, сходное положение создалось и в целом ряде других вузов по аналогичным или смежным специальностям. Выходом может послужить введение обязательного курса под названием «Математические основы информационной безопасности» (название может быть изменено). Курс должен читаться на 1-5 семестрах ПАРАЛЛЕЛЬНО курсу Высшей математики и включать в себя следующие разделы:

1 семестр: основные понятия, теория булевых функций;
2 семестр: алгебраические системы;
3 семестр: теория графов, теория автоматов;
4 семестр: комбинаторика, теория кодирования;
5 семестр: сложность вычислений и алгоритмов.

Тогда специализацию студентов можно было бы начинать с 4 курса, что безусловно повысит уровень подготовки выпускников.

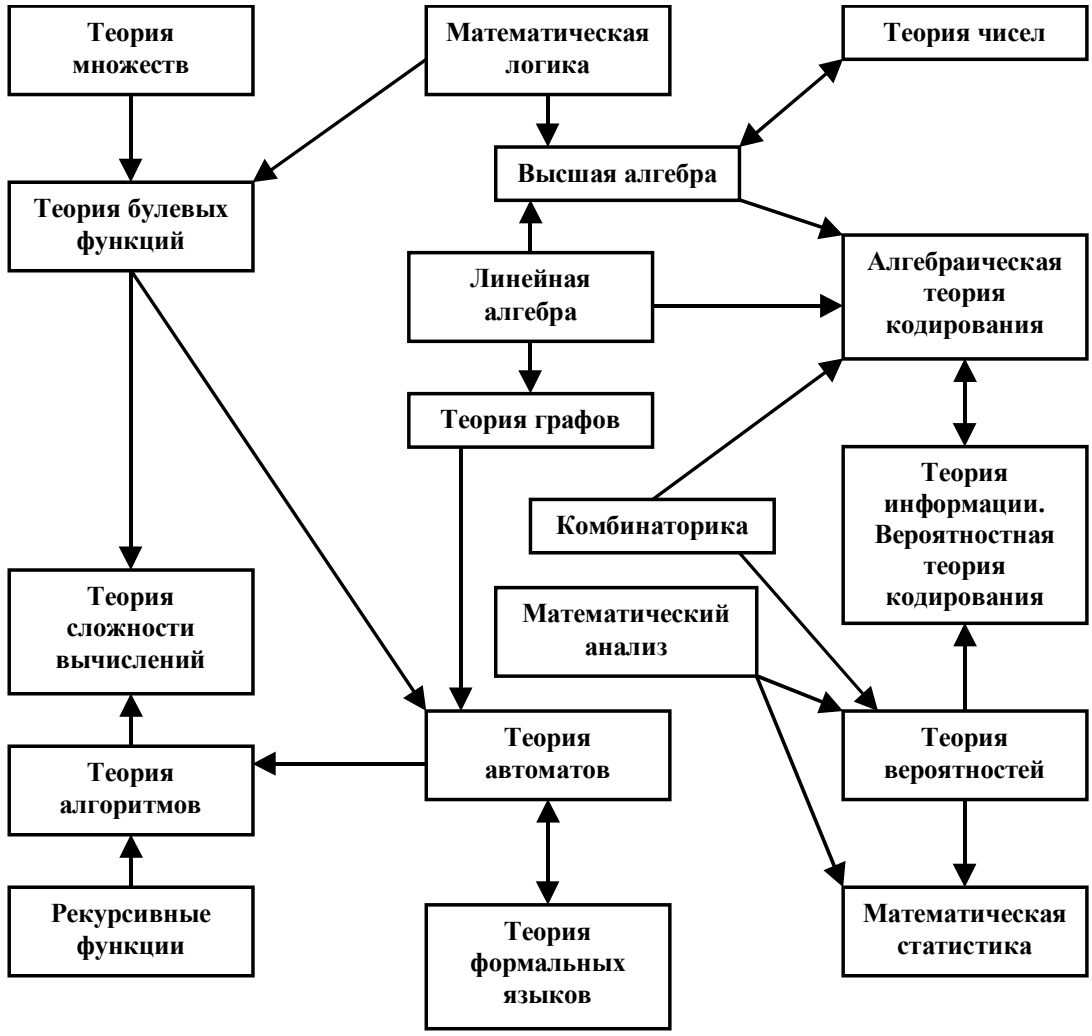

Рис. 1