

ОБ ОДНОЙ МЕТОДИЧЕСКОЙ ИНИЦИАТИВЕ Ю.С. БОГДАНОВА

Матвеев Г.В., Филиппов А.В.

Белорусский государственный университет, Минск, Беларусь
{matveev,filiptsov}@bsu.by

Во время руководства кафедрой высшей математики Юрий Станиславович Богданов уделял большое внимание вопросам методики преподавания математики. Под его руководством на кафедре работал методический семинар. Направления тем, предлагавшихся Ю.С. Богдановым к обсуждению на семинаре, затрагивали широкий круг вопросов, которые касались всех дисциплин, преподаваемых на кафедре: математический анализ, дифференциальные уравнения, аналитическая геометрия, алгебра. Большое внимание он уделял вопросам обновления программ дисциплин с целью расширения роли теоретического материала, имеющего актуальные приложения. В частности, после выхода из печати книги Г. Биркгофа и Т. Барти «Современная прикладная алгебра» [1] Ю.С. Богданов предложил рассмотреть на семинаре разделы алгебры и теории чисел, имеющие приложения к вопросам защиты информации, роль которых начала возрастать с развитием вычислительной техники, а также обсудить возможность преподавания их в БГУ. Работа, проведенная под руководством Ю.С. Богданова, впоследствии привела к ряду знаковых событий.

Кафедрой высшей математики было предложено внести в учебный план специальности «Информатика» дисциплину «Прикладная алгебра», в разработке которой и последующем преподавании принимали участие профессор В.С. Конюх и доценты В.М. Ширяев, Г.В. Матвеев, Д.Ф. Базылев. Особенностью этого курса являлось изучение не только классической теории чисел, но и ее приложений к современной криптографии, как представленных в книге Биркгофа и Барти, так и появившихся позднее: RSA-криптосистемы, DH-протокол, криптосистема Рабина. К сожалению, при переходе в 2013 году на сокращенные сроки обучения на специальности «Информатика» эта дисциплина была исключена из учебного плана. Однако часть материала, изучавшегося

в рамках этой дисциплины теперь присутствует в учебной программе дисциплины «Алгебра и теория чисел» на специальности «Прикладная информатика».

Впоследствии сотрудники кафедры Д.Ф. Базылев, М.М. Васьковский, Г.В. Матвеев, А.В. Филипцов принимали активное участие в разработке образовательного стандарта и учебных программ ряда дисциплин при открытии в БГУ новой специальности «Прикладная криптография». В частности, были разработаны учебные программы таких дисциплин, как «Криптографические системы с открытым ключом», «Линейные рекуррентные последовательности», «Базисы Гребнера», содержание которых относится к прикладной алгебре и теории чисел.

Надо отметить, что параллельно на кафедре математического моделирования и анализа данных были разработаны и читались дисциплины специализации по криптографическим приложениям алгебры и теории чисел. Опыт преподавания этих дисциплин нашел свое частичное отражение в объемном учебнике «Криптология» коллектива авторов во главе с Ю.С. Хариным [2].

На этом примере можно видеть, как методические инициативы Ю.С. Богданова оказали заметное влияние на изменения в учебном процессе на факультете прикладной математики и информатики.

Литература

1. Биркгоф Г., Барти Т. *Современная прикладная алгебра*. М.: Мир, 1976.
2. Харин Ю.С. [и др.]. *Криптология*. Мн.: БГУ, 2013.