УДК 51+378.147

Н.В. Неустроев
г. Великий Новгород, Россия

О ПРЕПОДАВАНИИ УЧЕБНОЙ ДИСЦИПЛИНЫ «ТЕОРИЯ ЧИСЕЛ С ПРИЛОЖЕНИЯМИ В КРИПТОГРАФИИ» СТУДЕНТАМ 4 КУРСА ПО НАПРАВЛЕНИЮ ПОДГОТОВКИ 01.03.01 МАТЕМАТИКА НАПРАВЛЕННОСТИ МАТЕМАТИКА В ОБРАЗОВАНИИ, ФУНДАМЕНТАЛЬНЫХ И ПРИКЛАЛДНЫХ ИССЛЕДОВАНИЯХ

Аннотация. В статье раскрываются некоторые особенности преподавания учебной дисциплины «Теория чисел с приложениями в криптографии» для студентов 4 курса с использованием технологии модульно-рейтингового обучения и с использованием ин-

формационных технологий при организации коммуникации со студентами и мультимедиа средств при проведении лекционных и практических занятий.

Ключевые слова: преподавание, методические рекомендации, мультимедиа средства.

Организация изучения учебной дисциплины

Образовательный процесс по учебной дисциплине формируется с использованием технологии модульно–рейтингового обучения.

Реализация интегральной модели образовательного процесса по модулю предполагает использование следующих технологий стратегического уровня (задающих организационные формы взаимодействия субъектов образовательного процесса), осуществляемых с использованием определенных тактических процедур:

– лекционные (вводная лекция, информационная лекция, проблемная лекция; обзорная лекция; рефлексия);

– практические (моделирование; работа в малых группах);

– самоуправления (самостоятельная работа студентов) (работа с источниками по темам дисциплины, моделирование процессов, выполнение индивидуальных заданий).

Рекомендуется использование информационных технологий при организации коммуникации со студентами для представления информации, выдачи рекомендаций и консультирования по оперативным вопросам (электронная почта), использование мультимедиа средств при проведении лекционных и практических занятий.

Методические рекомендации по организации изучения учебной дисциплины «Теория чисел с приложениями в криптографии»

1. Элементы теории делимости и теории сравнений (см. [1], [3])

Теория чисел – это необходимый арсенал разработчика или аналитика данных, но в ее освоении студентам придется столкнуться со сложностями, преодолимыми только при системном подходе.

Замечательный английский математик Г.Х. Харди утверждал, элементарную теорию чисел следует считать одним из лучших предметов для первоначального математического образования. Она требует очень мало предварительных знаний, а предмет ее понятен и близок. Методы рассуждений, принимаемые, ею просты, общи и немногочисленны; среди математических наук нет равной ей в обращении к естественной человеческой любознательности. Зачастую решение ее задач требует математической изобретательности, преодоления значительных трудностей, отыскания новых методов и идей, находящих продолжение в современной математике. Теория чисел является наукой о числовых

системах с их связями законами. При этом в первую очередь уделяется внимание числам натурального ряда, которые являются основой для построения других числовых систем: целых, рациональных и иррациональных, действительных и комплексных, кватернионов и других гиперкомплексных чисел.

2. Содержание учебной дисциплины

Введение. Элементы теории делимости и теории сравнений.

Раздел № 1 Теоретико-числовые алгоритмы.

1.1. Тестирование целых чисел на простоту.

1.2. Факторизация целых чисел.

Раздел № 2 Основы симметрической криптографии.

2.1. Шифрование. Многоалфавитные шифры замены. Шифрование с автоключом.

2.2.Блочные шифры. Американский стандарт шифрования данных. Российский стандарт шифрования.

Раздел № 3 Основы асимметричной криптографии.

3.1. Открытое распределение ключей.

3.2. Цифровая электронная подпись.

3.3. Система RSA.

Содержательно рассмотреть и на примерах показать приложения теории чисел в криптографии: сложность арифметических операций, проверка чисел на простоту, дискретное логарифмирование, криптосистемы с закрытым и открытым ключом, атаки на криптосистемы (см. [2, с. 180–187]).

На дом после каждого практического занятия задаются те примеры, аналоги которых разработаны в аудитории, а также примеры, требующие самостоятельного поиска путей решений в соответствии с рассмотренной теорией.

Темы самостоятельных работ представлены ниже. Отчет о проделанной самостоятельной работе и домашние работы представляются в виде конспекта или презентации.

Освоение каждой темы, включенной в программу учебной дисциплины, предусматривает овладение студентами всех затронутых в нее понятий, теорем и их доказательств, методов и приемов решения соответствующих примеров и задач. Основными источниками, которые могут быть использованы, являются, в первую очередь, лекции преподавателя, а также учебники, задачники, указанные в рабочей программе. Полезными будут учебники из дополнительной литературы рабочей про-

граммы, а также другая литература, которую студент может подобрать самостоятельно. Занятия проводятся, как правило, в диалоговой форме: в ходе лекций преподавателем систематически задаются вопросы студентам, на практических занятиях проводится опрос по пройденному материалу, преподавателем даются образцы решения типовых задач и т.п. После изучения каждой темы на лекционных и практических занятиях проводится небольшая практическая аудиторная самостоятельная работа, результаты которой учитываются в ходе рубежной аттестации. По завершению изучения каждого раздела проводится итоговая контрольная работа (КР). Основной задачей преподавателя является ознакомление студентов с математическими методами, применяемыми в смежных разделах математики. Технологически эти задачи решаются с помощью информационных лекций, практических занятий, ответов на вопросы студентов, обсуждений результатов решения задач, самостоятельной работы студентов.

Темы домашнего задания:

1 Алгоритм Миллера.

2 Вероятностные тесты на простоту.

3 Метод Ферма. Методы Полларда.

4 Метод гаммирования.

5 Композиция шифров.

6 Система защиты информации на основе заданного рюкзака.

7 Обобщенная рюкзачная криптосистема с открытым ключом.

8 Временные оценки относительно трудоемкости арифметических операций.

Данная тематика автором используется для ВПР (выпускная квалификационная работа, например: разработать элективный курс для школьников 9-11 классов «Элементы теории чисел с приложениями в криптографии»), а также в проектной деятельности (так например : проекты «Арифметические алгоритмы в криптографии» и «Теоретико-числовые методы в криптографии»).

Список использованной литературы

1. Неустроев, Н. В. Теория чисел: книга для студентов специальности «учитель математики», «прикладная математика», «ПОВТ» / Н. В. Неустроев. – Великий Новгород : НовГУ им. Ярослава Мудрого, 2004. – 161 с.
2. Неустроев, Н. В. Элементы прикладной теории чисел: учебное пособие для специальности «учитель математики», «прикладная математика», «ПОВТ» / Н. В. Неустроев, О. Н. Неустроева. – Великий Новгород : НовГУ им. Ярослава Мудрого, 2007. – 189 с.

3. Неустроев, Н. В. Теория чисел: книга для студентов специальности Педагогическое образование (Математика и информатика) / автор-составитель Н. В. Неустроев. – Великий Новгород : НовГУ им. Ярослава Мудрого, 2018. – 276 с.