УДК 004.056

ОБ ОСОБЕННОСТЯХ ПРЕПОДАВАНИЯ МАТЕМАТИЧЕСКИХ ОСНОВ ЗАЩИТЫ ИНФОРМАЦИИ В ВОЕННОМ ВУЗЕ

Л.В. Михайловская, Е.В. Валаханович, Е.В. Жалобкевич

В XXI веке растет количество специальностей в ВТУЗах, призванных обслуживать различные информационные системы и технологии. В учебном процессе увеличивается удельный вес соответствующих курсов и дисциплин. Их преподавание требует применения новых разделов высшей математики и совершенствования существующих методик.

Бурное развитие со второй половины XX века нанотехнологий, цифровых систем связи, средств вычислительной техники привело человеческое общество в новую технологическую эпоху, которую многие называют «информационной». Возникло поколение принципиально новых – информационных технологий, преобразивших все аспекты жизни нашей цивилизации, в том числе и сферу военной деятельности.

Применение информационных технологий без должного внимания к вопросам защиты информации прежде всего в военной сфере может иметь крайне негативные последствия. Неправомерное искажение, уничтожение или разглашение определенной части информации, равно как и дезорганизация процессов ее обработки и передачи в автоматизированных системах обработки информации могут привести к серьезному материальному и моральному урону.

Высокий профессиональный уровень, которому должен соответствовать современный военный инженер в сфере информационных технологий и их приложений, предполагает твердое владение соответствующими математическими методами и навыками по их использованию.

В настоящее время на изучение классического курса высшей математики в учреждении образования «Военная академия Республики Беларусь» для подготовки военных специалистов-инженеров отводится 396 часов, включая тему «Теория вероятностей и математическая статистика». Безусловно, данного объема часов недостаточно для обеспечения овладения новыми разделами математики, которые предполагает современный уровень развития материально-технической базы Вооруженных Сил. Обучение высшей математике должно включать в себя не только базовый (классический) курс, но и изучение дополнительных прикладных разделов математики с учетом будущей профессиональной деятельности курсантов.

Выпускники специальностей «Телекоммуникационные системы (эксплуатация)», «Эксплуатация автоматизированных систем обработки информации», «Телекоммуникационные системы (радиоэлектронная борьба, радиоэлектронная разведка)», «Авиационные радиоэлектронные системы» должны быть профессионально подготовлены в области основных исторических, теоретических и методологических положений передачи, хранения и защиты информации как от помех, так и от несанкционированного

доступа. Также им необходимо обладать практическими навыками применения современных алгоритмов криптографической защиты информации.

В связи с этим в 2010 году на кафедре высшей математики учреждения образования «Военная академия Республики Беларусь» был разработан и внедрен факультативный курс «Защита информации», состоящий из пяти базовых тем, всего 28 часов практических и/или лабораторных работ.

На основе этого курса разработана учебная программа по дисциплине «Прикладная математика» для курсантов специальностей «Телекоммуникационные системы (эксплуатация)», «Эксплуатация автоматизированных систем обработки информации», «Телекоммуникационные системы (радиоэлектронная борьба, радиоэлектронная разведка)».

На курс прикладной математики, включающий в себя лекции, практические занятия, лабораторные работы, расчетно–графическую работу по теме «Алгоритмы криптографической защиты информации» и дифференцированный зачет, отводится 76 часов.

Целью изучения учебной дисциплины является обучение основным математическим методам теории чисел, теории групп, колец и полей, конечных полей для их последующего использования в защите информации как от помех так и от несанкционированного доступа, в цифровой обработке сигналов и изображений, в помехоустойчивом кодировании и ряде других важных задач, решаемых в военно-инженерной деятельности.

Особенность преподавания курса «Прикладная математика» в ВА РБ состоит в использовании информационных технологий в области программирования и в индивидуальном подходе к курсантам.

В криптографии ведется работа с числами длиной десять и более десятичных знаков, вычисления с которыми отнимают много времени и сил. В этой связи преподавателями кафедры высшей математики разработан ряд алгоритмов и мини-программ, в частности для решения линейных, квадратных уравнений, а также систем линейных уравнений в кольцах классов вычетов.

Курсанты распределены на три подгруппы в зависимости от их уровня подготовки. Исходя из качества выполнения заданий возможен переход из одной подгруппы в другую.

Курсанты первой подгруппы выполняют упрощенные задачи с применением готового программного продукта.

Для курсантов второй подгруппы подбираются задания базового уровня или задания с дополнительными условиями, которые требуют не только умения использовать готовое программное обеспечение, но и разрабатывать свои алгоритмы для решения поставленной задачи.

Курсантам третьей подгруппы предлагаются задания, требующие хорошей математической подготовки, самостоятельного поиска решения, исследовательской деятельности и разработки мини-программ. Курсанты именно третьей подгруппы максимально усваивают преподаваемый материал, проходят все этапы осмысления, способны к самостоятельному творчеству.

Важным аспектом данного подхода является то, что для реализации конкретной задачи при помощи программных средств курсантам необходимо мыслить в нескольких направлениях: как реализовать алгоритм математически и как сделать его понятным для машины. Такой метод, как правило, значительно сокращает время решения поставленной задачи.

В большинстве случаев алгоритмы реализованы «на скорую руку» в консоле, в них не обработаны исключения и нет привычного для пользователей ПК интерфейса, т.к. они предназначены для личного пользования. Данные мини-программы не реализуют алгоритм шифрования, а лишь облегчают определенные этапы вычислений.

Исходя из этого, каждая лабораторной работа предполагает оформление отчета в формате таблицы Excel. Отчет состоит из трех частей: указания к выполнению, непосредственно сам отчет и лист проверки выполнения. В указаниях отмечаются способы решения задач (вручную, написание мини-программ, использование инженерного калькулятора, ПК, использование ресурсов табличного процессора Excel). Выбор технических средств для решения предоставлен обучающимся и зависит от уровня успеваемости курсантов.

Конечным результатом изучения дисциплины «Прикладная математика» является умение курсантов вскрывать классические криптографические тексты, вскрывать учебные, современные криптограммы.

На кафедре высшей математики ВА РБ коллективом авторов (Липницкий В. А., Михайловская Л. В., Валаханович Е. В.) разработан практикум «Защита информации» [1]. Книга отражает с практической точки зрения темы «Основы теории чисел», «Классы вычетов», «Историческая криптография», «Современные криптографические системы: криптосистема RSA и криптосистема Эль Гамаля», позволяет практически освоить материал пособия [2]. Изучаемые темы разработаны по одной схеме: сначала идет изложение необходимого теоретического материала, затем разбирается решение типичных для данной темы задач и, наконец, предлагаются задания по вариантам для выполнения конкретной самостоятельной или лабораторной работы. Следует отметить, что в последних двух темах продолжается углубление в основы теории чисел – изучается китайская теорема об остатках, квадратичные вычеты и их свойства. Приведенные решения типовых задач по изучаемой теме делают материал доступным для понимания, облегчают его усвоение обучаемыми, в том числе и при самостоятельной работе.

В настоящее время разрабатывается пособие по прикладной математике, включающее в себя 12 лабораторных работ: одна работа посвящена древнейшим криптосистемам, которые как нельзя лучше показывают становление современной криптографии: переход от буквенных шифров к математическим основам защиты информации; три последующие – теории чисел, в частности, теории классов вычетов, которая является основой для освоения криптосистемы RSA и Рабина; работы по теории групп, колец и полей связаны с криптосистемой Эль Гамаля, теорией норм синдромов, полями Галуа. Данный комплекс лабораторных работ готовит обучающихся к изучению

следующей криптосистемы (стандарту шифрования), требующей более сложной математики – криптосистеме AES.

Знание математических основ защиты информации в автоматизированных системах обработки информации необходимо для действенного усвоения всего спектра алгоритмов и сути современных криптосистем, с которыми придется столкнуться в своей практической деятельности будущим специалистам-инженерам.

Список литературы

1. Липницкий, В.А. Защита информации: практикум / В.А. Липницкий, Л.В. Михайловская, Е.В. Валаханович. – Минск: ВА РБ, 2012. – 86 с.
2. Липницкий, В.А. Современная прикладная алгебра. Математические основы защиты информации от помех и несанкционированного доступа / В.А. Липницкий. – Минск: БГУИР, Учебно-методическое пособие. – 2-е изд. – Мн., 2006. – 88 с.

Михайловская Людмила Вячеславовна, доцент кафедры высшей математики ВА РБ, кандидат физико-математических наук, доцент, ludmila_mi@mail.ru

Валаханович Екатерина Валентиновна, преподаватель кафедры высшей математики ВА РБ, магистр технических наук, ekat.valah@gmail.com

Жалобкевич Екатерина Витальевна, преподаватель кафедры высшей математики ВА РБ, магистр технических наук, beluzhka@gmail.com