

О НЕКОТОРЫХ ТЕНДЕНЦИЯХ ПРЕПОДАВАНИЯ ПРИКЛАДНОЙ МАТЕМАТИКИ В ВОЕННОМ ВУЗЕ

Военная академия Республики Беларусь

Михайловская Л.В., Валаханович Е.В., Липицкий В.А.

Бурное развитие со второй половины XX века микро- и нанотехнологий, средств вычислительной техники, компьютерных и инфокоммуникационных систем (ИКС) привело общество в новую, «информационную», эпоху. Возникло поколение принципиально новых – информационных технологий, преобразивших все аспекты жизни нашей цивилизации.

Информационная эпоха нашла отражение в сфере военной деятельности. Новейшие военные стратегии предполагают в будущих военных конфликтах первоочередное уничтожение или парализацию ИКС противника, реальные боевые действия предваряет настоящая информационная война для полной дестабилизации и дезориентации противника.

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

Высокий профессиональный уровень, которому должен соответствовать современный военный инженер, невозможен без твердого владения соответствующими математическими методами в сфере защиты информации.

Соответственно, обучение высшей математике в военных ВУЗах 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» Военной Академии должны быть профессионально подготовлены в области основных положений передачи, хранения и защиты информации, как от помех, так и от несанкционированного доступа. Также военным специалистам 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 курс «Защита информации». На данном этапе на

основе названного курса разработана и внедрена в учебный процесс программа по дисциплине «Прикладная математика».

На данную дисциплину отводится 76 часов, что включает в себя лекции, практические занятия, лабораторные работы, расчетно–графическую работу по теме «Алгоритмы криптографической защиты информации» и дифференцированный зачет.

Целью изучения данной 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 в ряде других важных задач, решаемых в военно-инженерной деятельности; освоение курсантами основных алгоритмов классической и современной криптографической защиты информации; освоение обучаемыми математических методов формирования и обработки помехоустойчивых кодов.

Особенности преподавания курса «Прикладная математика» в УО «ВА РБ» состоят в существенном использовании информационных технологий из области программирования и в индивидуальном подходе к курсантам. Так, преподавателями кафедры высшей математики УО «ВА РБ» разработан цикл из 11 лабораторных работ, в которых рассматриваются основные темы криптографии: от алгоритмов вычисления наибольшего делителя двух целых чисел до декодирования двукратных ошибок в примитивных двоичных БЧХ-кодах. Данные ЛР снабжены множеством разного рода подпрограмм и мини-программ. В частности, алгоритмами решения линейных и квадратных уравнений в полях Галуа, адаптированными алгоритмами для решения систем линейных уравнений в кольцах классов вычетов как по простому, так и по составному модулю. Данные мини-программы облегчают определенные этапы вычислений.

Для практического освоения изучаемой дисциплины «Прикладная математика» на лабораторных занятиях 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, а также задания с дополнительными условиями, которые требуют не только умения использовать готовое программное обеспечение, но и разрабатывать свои индивидуальные алгоритмы для решения поставленной задачи.

Курсантам третьей подгруппы предлагаются задания, требующие хорошей математической подготовки, самостоятельного поиска

решения, исследовательской деятельности и навыков разработки мини-программ. Курсанты именно третьей подгруппы максимально усваивают преподаваемый материал, проходят все этапы осмысления курса, именно они способны к самостоятельному творчеству.

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, работать с линейными помехоустойчивыми кодами, кодами Хемминга, БЧХ-кодами.

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.

Литература:

1. Липницкий В. А., Михайловская Л. В., Валаханович Е. В. Защита информации: практикум. – Минск: ВА РБ, 2012. – 87с.
2. Липницкий, В. А. Современная прикладная алгебра. Математические основы защиты информации от помех и несанкционированного доступа: учеб. метод. пособие. – Минск, 2006. – 88 с.

СОВРЕМЕННЫЕ СПОСОБЫ ПРЕПОДАВАНИЯ В ВОЕННОМ УЧЕБНОМ ЗАВЕДЕНИИ

Военная академия Республики Беларусь

Банников В.Ю., Цыганков В.Н.

Одна из задач совершенствования образовательного процесса в военном вузе – максимально приблизить обучение к запросам времени, помочь раскрытию всех дарований личности курсанта и, в конечном счете, подготовить специалиста, сочетающего в себе широкую фундаментальную научную подготовку с глубокими всесторонними знаниями конкретной специальности, убежденного в необходимости добросовестного служения Родине. Помимо обладанием высоким уровнем военной и инженерной квалификации, он должен быть челове-