УДК 004.056

О СПЕЦИФИКЕ ПРЕПОДАВАНИЯ ОСНОВ ЗАЩИТЫ ИНФОРМАЦИИ ПО ПРОГРАММЕ ПРИКЛАДНОЙ МАТЕМАТИКИ В ВОЕННОЙ АКАДЕМИИ

Е.В. Валаханович

Учреждение образования «Военная академия Республики Беларусь», Минск, Беларусь

Аннотация. В настоящее время информация стала одним из ключевых ресурсов государства. Вместе с ростом значимости информации возрастают и риски, связанные с несанкционированным доступом и кибератаками. В этих условиях подготовка квалифицированных специалистов в области защиты информации становится одной из приоритетных задач для всех сфер деятельности.

Ключевые слова: защита информации; информационная безопасность; шифрование; кодирование; алгоритм; математические методы.

ON THE SPECIFICS OF TEACHING THE FUNDAMENTALS OF INFORMATION SECURITY ACCORDING TO THE APPLIED MATHEMATICS CURRICULUM OF THE MILITARY ACADEMY

E.V. Valakhanovich

The Military Academy of the Republic of Belarus, Minsk, the Republic of Belarus

Abstract. Currently, information has become one of the key sovereign resources. However, risks associated with an unauthorized access and cyberattacks surge as the value of information increases. In view of the above, training of qualified information security specialists has become one of the priorities for all areas of activity.

Keywords: data protection; information security; encryption; coding; algorithm; mathematical methods.

Введение

Сегодня, в эпоху цифровой трансформации, информация стала одним из ключевых ресурсов, определяющих успех как отдельных отраслей деятельности, так и государств в целом. Однако вместе с ростом значимости информации возрастают и риски, связанные с несанкционированным доступом и кибератаками. В этих условиях подготовка квалифицированных специалистов в области защиты информации становится одной из приоритетных задач для всех сфер деятельности.

Основная часть

Специалисты по информационной безопасности необходимы практически во всех отраслях: от финансов и здравоохранения до энергетики и обороны. Они обеспечивают защиту данных, предотвращают утечки информации, разрабатывают системы шифрования и мониторинга, а также участвуют в создании нормативно-правовой базы, регулирующей вопросы информационной безопасности.

Учитывая специфику деятельности Вооруженных Сил, многоуровневая система управления должна обеспечить слаженную работу разнородных подразделений, выполняющих задачи на различных направлениях, в режиме реального времени. При этом противник не должен вскрыть или подавить прохождение информации по каналам связи. Это означает, что в военном деле решение вопросов защиты информации должно быть организовано с наивысшим приоритетом. Неправомерное искажение, уничтожение или разглашение определенной части информации, равно как и дезорганизация процессов ее обработки и передачи, могут привести к серьезным последствиям.

В связи с вышеизложенным, современный военный инженер должен обладать высоким профессиональным уровнем базовой подготовки в сфере защиты информации, включающим твердое владение специальными математическими методами и навыками по их использованию.

В настоящее время в учреждении образования «Военная академия Республики Беларусь» на изучение курса высшей математики отводится 360 часов. Вне всякого сомнения, этого объема часов по высшей математике недостаточно для выполнения требований по обеспечению базовой подготовки инженера, которые предъявляет современный уровень развития материально-технической базы Вооруженных Сил. Обучение высшей математике должно включать в себя не только базовый курс, но и изучение специальных прикладных разделов математики с учетом будущей профессиональной деятельности курсантов.

Выпускники ряда специальностей должны обладать профессиональными теоретическими знаниями по передаче, хранению и защите информации, как от помех, так и от несанкционированного доступа, а также практическими навыками применения современных алгоритмов криптографической защиты информации.

Для их специальной подготовки разработана учебная программа по дисциплине «Прикладная математика» в объеме 76 часов, включающая в себя лекции, практические занятия, лабораторные и контрольную работу по теме «Алгоритмы криптографической защиты информации» и дифференцированный зачет.

В ходе изучения «Прикладной математики» курсанты овладевают основными математическими методами теории чисел, теории групп, колец и полей, конечных полей для их последующего использования в защите и цифровой обработке информации, в помехоустойчивом кодировании и в ряде других важных задач, решаемых в военно-инженерной деятельности; основными алгоритмами современной криптографической защиты информации; математическими методами 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.

В криптографических алгоритмах ведется работа с числами длиной от нескольких до десятков и сотен десятичных знаков, вычисления с которыми отнимают много времени и сил. Даже простейшие теоретико-числовые алгоритмы становятся непреодолимыми для точной обработки их вручную. Это составляет существенную проблему в реализации любого курса математических основ защиты информации.

В связи с этим преподаватели кафедры высшей математики УО «ВА РБ» разработали цикл из 11 лабораторных работ. Если в первой из них рассматриваются алгоритмы вычисления наибольшего делителя двух целых чисел, то в последней из них декодируются двукратные ошибки в примитивных двоичных БЧХ-кодах с конструктивным расстоянием 5 решением квадратных уравнений в поле Галуа – поле

определения рассматриваемого БЧХ-кода. Данные ЛР снабжены множеством разного рода алгоритмов, 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.

Для практического освоения лабораторных занятий 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.

Важным аспектом данного подхода является то, что для реализации конкретной задачи при помощи программных средств курсантам необходимо мыслить в нескольких направлениях: какой алгоритм нужен, как реализовать этот алгоритм математически, как сделать нужный алгоритм понятным для компьютера. Такой метод, как правило, значительно сокращает время решения поставленной задачи. И главное, развивает творческую инициативу курсантов.

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.

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.

В ходе обучения дисциплине «Прикладная математика» применяется 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].

Кроме того, в настоящее время коллективом авторов разработано и передано для издания учебно-методическое пособие «Прикладная математика. Лабораторные работы. Практикум» 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 будет готовить обучающихся к изучению стандарту шифрования, требующего более сложной математики – криптосистеме AES.

Заключение

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.

Подготовка специалистов в области защиты информации – важнейшая задача, от решения которой зависит безопасность данных, конфиденциальность и устойчивость современных систем. Для успешной реализации задачи по подготовке специалистов в области защиты информации требуется системный подход, учет современных тенденций и активное внедрение инновационных технологий в образовательный процесс.

Список использованных источников

1. Липницкий В. А., Михайловская Л. В., Валаханович Е. В. (2012) *Защита информации: практикум*. Минск: ВА РБ.

2. Липницкий В. А. (2006) *Современная прикладная алгебра. Математические основы защиты информации от помех и несанкционированного доступа*. Минск: БГУИР.

References

1. Lipnitski V. A., Mikhailovskaya L. V., Valakhanovich E. V. (2012) *Information protection: workshop*. Minsk: MA RB.

2. Lipnitski V. A. (2006) *Modern applied algebra. Mathematical foundations for protecting information from interference and unauthorized access*. Minsk: BSUIR.

Сведения об авторах

Валаханович Е. В., старший преподаватель, Учреждение образования «Военная академия Республики Беларусь», ekat.valah@gmail.com.

Information about the authors

Valakhanovich E. V., senior lecturer, The Military Academy of the Republic of Belarus, ekat.valah@gmail.com.