УДК 511:003.26

Н. В. Сакович, Е. В. Гусева,
г. Могилев, Беларусь

О КУРСЕ «МАТЕМАТИЧЕСКИЕ ОСНОВЫ ЗАЩИТЫ ИНФОРМАЦИИ» ДЛЯ СТУДЕНТОВ СПЕЦИАЛЬНОСТИ «ФИЗИКА И ИНФОРМАТИКА»

При изучении учебной дисциплины для понимания сути алгоритмов, понимания как они работают, необходимы знания по алгебре и теории чисел. В связи с отсутствием в учебном плане практических занятий по дисциплине и отсутствием профессиональных компетенций в области теории чисел необходима организация аудиторной и внеаудиторной работы студентов.

Ключевые слова: криптография, криптосистемы, теория чисел, простые числа, числовые сравнения, классы вычетов, конечные поля, теорема Эйлера.

Дисциплина «Математические основы защиты информации» играет важную роль в профессиональной и общенаучной подготовке студентов специальности 1–02 05 02 «Физика и информатика».

Математические основы защиты информации — область математики, изучающая вопросы, связанные с сохранением и передачей информации. Достоверность и надежность получаемой информации, защищенность ее от несанкционированного доступа весьма актуальна. Актуальность проблемы, связанной с обеспечением информационной безопасности, с те-

Электронный архив библиотеки МГУ имени А.А. Кулешова

чением времени все более усиливается. Защиту информации можно осуществить ограничением доступа к информации или криптографическим преобразованием информации, или шифрованием. Криптография занимается поиском и исследованием новых способов зашифровывания информации. Криптоанализ же, в свою очередь, изучает способы расшифровывания информации без знания ключей и алгоритмов шифрования. Современная криптография состоит из четырех крупных разделов:

1. Симметричные криптосистемы.
2. Криптосистемы с открытым ключом.
3. Системы электронной подписи.
4. Управление ключами [1].

При изучении дисциплины «Математические основы защиты информации», которая позволяет ознакомиться с историей криптографии, различными приемами шифрования, основами современных методов шифрования, с оценкой сложности отдельных детерминированных алгоритмов, для понимания сути алгоритмов, понимания как они работают, необходимы знания по алгебре и теории чисел.

В традиционной криптографии с несложными преобразованиями (простая замена, перестановка, гаммирование) не было необходимости применять глубокие результаты теории чисел. Ситуация изменилась с появлением криптосистем с открытым ключом, в основе которых лежат односторонние преобразования, например, операция возведения в степень по огромным модулям.

В криптографии сообщения представляются символами некоторого конечного алфавита. Этим символам ставят в соответствие числа от 0 до N–1, где N — число элементов (мощность) алфавита. Поэтому шифрование и расшифровывание сообщений представляют собой преобразование натуральных чисел, меньших N. В процессе переработки информации приходится выполнять те или иные арифметические действия или преобразования. При этом возникает задача эффективных приемов выполнения этих действий и оценки сложности алгоритмов, реализующих криптопреобразования.

Особую роль играют простые числа. Это касается задач факторизации, задач проверки простоты числа, алгоритма нахождения всех простых чисел, не превосходящих заданного числа, задач о распределении простых чисел в натуральном ряде. При построении современных криптосистем требуются очень большие простые числа. Нужно подчеркнуть значимость теоремы о делении с остатком, алгоритма Евклида, нахождения наибольшего общего делителя двух натуральных чисел, а также теории непрерывных цепных дробей.

Электронный архив библиотеки МГУ имени А.А. Кулешова

Ввиду конечности алфавитов сообщений важную роль играет раздел теории чисел — теория сравнений, в которой числа, имеющие одинаковые остатки от деления на фиксированное число (модуль), считаются одинаковыми. В качестве модуля естественно выбрать мощность алфавита сообщений. Для изложения методов шифрования без передачи ключей, с открытым ключом, электронной подписи необходимо знание методов решения сравнений первой степени и систем таких сравнений, а также свойств классов вычетов по простому и составному модулю, знание теорем Эйлера и Ферма. Для усвоения материала необходимо знание китайской теоремы об остатках. Алгоритмы современной защиты информации криптосистемы RSA, Эль Гамаля, Рабина основаны на вычислениях в кольцах классов вычетов. Для решения криптографических задач необходимо знание понятий теории групп, особенно теории групп подстановок, фактор-группы, теоремы Лагранжа. Объектами преобразований в криптографии являются не только вычеты по простому модулю, но и более сложные образования — конечные поля [2].

Планирование и организация времени, отведенного на изучение дисциплины, определяются видами занятий и их продолжительностью. При изучении учебной дисциплины в рамках названной специальности и студенты, и преподаватель сталкивается с определенными трудностями. При изложении курса используется материал из курса «Алгебра и геометрия». «Теория чисел», как отдельная дисциплина, в соответствии с учебным планом этой специальности студентами не изучается. На изучение дисциплины «Математические основы защиты информации» отводится 20 аудиторных часов, из них 20 часов лекций.

В связи с отсутствием в учебном плане практических занятий по данной дисциплине и отсутствием профессиональных компетенций в области теории чисел необходима организация аудиторной и внеаудиторной работы студентов. Нами разработаны презентационные и дидактические материалы, которые включают краткий теоретический материал, рассмотрение алгоритмов, примеры решения заданий и задания для самостоятельного выполнения, а также дополнительный справочный материал.

Список использованной литературы:

1. Нечаев, В. И. Элементы криптографии. Основы теории защиты информации / В. И. Нечаев. – Москва : Высшая школа, 1999. – 109 с.
2. Орлов, В. А. Теория чисел в криптографии : учеб. пособие / В.А. Орлов, Н.В. Медведев, Н. А. Шимко, А. Б. Домрачева. – Москва : Издательство МГТУ им. Н. Э. Баумана, 2011. – 223 с.

Электронный архив библиотеки МГУ имени А.А. Кулешова