УДК 004.056

И.В. Лысенко

Национальный аэрокосмический университет имени Н.Е. Жуковского «ХАИ», Харьков

О МАТЕМАТИЧЕСКОЙ ПОДГОТОВКЕ СТУДЕНТОВ, ОБУЧАЮЩИХСЯ ПО СПЕЦИАЛЬНОСТИ «КИБЕРБЕЗОПАСНОСТЬ»

Сформулированы предложения и рекомендации относительно содержания и преподавания математических и математически ориентированных дисциплин студентам, обучающимся по специальности «Кибербезопасность». Рассмотрены разделы математики, необходимые для изучения дисциплин, формирующих выпускника-бакалавра или магистра в области информационной безопасности. Обоснована целесообразность использования систем компьютерной математики в процессе изучения математически ориентированных дисциплин.

Ключевые слова: *кибербезопасность, криптология, системы компьютерной математики.*

Введение

Вопрос важности и актуальности математической подготовки современного специалиста в области информационных технологий (ИТ) не требует обоснований, а поскольку кибербезопасность представляет собой одну из важных компонент ИТ, то это касается и собственно кибербезопасности.

Вполне очевидно, что подготовка бакалавров и магистров по всем специальностям, входящим в направление «Информационные технологии», предполагает существование некоего общего для них ядра математических и математически ориентированных дисциплин (например, такие разделы дискретной математики, как теория множеств, теория графов, комбинаторика; теория вероятностей и математическая статистика; теория информации и кодирования и др.). В то же время, специфика каждой специальности обусловливает необходимость, как делать акценты на некоторых из тех разделов математики, которые входят в упомянутое «ядро», так и изучать те её разделы, знание которых не является необходимым для других специальностей.

В этой связи **цель статьи** состоит в том, чтобы сформулировать предложения и рекомендации относительно содержания и преподавания математических и математически ориентированных дисциплин студентам, обучающимся по специальности «Кибербезопасность».

О преподавании математических и математически ориентированных дисциплин

Деление дисциплин на математические и математически ориентированные – вполне естественно, если под первыми понимать дисциплины из категории «чистой» математики, а под вторыми – те из них, которые имеют прикладное значение и в их основе лежат те или иные понятия, разделы, направления математики «чистой». Примерами первой могут быть «Теория чисел» и «Высшая алгебра», а второй – «Теория информации и кодирования» и «Теория принятия решений» (или «Исследование операций»).

К числу основных дисциплин, формирующих облик *бакалавра* в области кибербезопасности, относятся: «Системы технической защиты информации», «Управление информационной безопасностью», «Комплексные системы защиты информации», «Прикладная криптология», «Защита информации в телекоммуникационных системах», «Антивирусная защита». Математически ёмкой (в нашей терминологии – математически ориентированной) среди них является «Прикладная криптология». То же самое можно сказать и о дисциплине «Теория информации и кодирования», изучение которой предшествует изучению таких курсов, как «Системы технической защиты информации», «Аппаратные средства защиты информации», «Защита информации в телекоммуникационных системах».

Изучение курса «Прикладная криптология» в части, касающейся изучения механизмов *несимметричной* криптографии и криптоанализа, подразумевает знакомство с теоретико-числовой и алгебраической проблематикой. В этой связи представляется целесообразным рассматривать два отдельных курса: «Основы элементарной теории чисел и теоретико-числовые методы в криптологии» и «Основы теории алгебраических систем». Что касается содержания первого из них, то оно должно включать не только базовые сведения из элементарной теории чисел, а именно: основные теоретико-числовые функции, основы теории сравнений первой степени и систем сравнений первой степени, основы теории квадратичных вычетов и сравнений второй степени, основы теории первообразных корней и индексов, но также и вопросы теоретико-числовой проблематики, относящиеся к криптологии: алгоритмы факторизации и дискретного логарифмирования, генерации и проверки простоты чисел. Содержанием второго из упомянутых курсов должно быть: основы теории групп, колец и конечных полей, основы тео-

рии эллиптических кривых, основы теории векторных пространств, основы теории решёток, булева алгебра, а также матроиды.

Так, необходимость изучения основ теории решёток обусловлена тем, что в связи с успехами квантового компьютинга и связанными с этим практическими следствиями, а именно – возможностями решения задач факторизации и дискретного логарифмирования за полиномиальное время и, соответственно, компрометации криптосистем на их основе (RSA, ElGamal, Diffie-Hellman), возрастает роль алгоритмов так называемой постквантовой криптографии, в основу стойкости которых положены математические задачи, для решения которых за полиномиальное время не существует алгоритмов для квантового компьютера. Одной из таких задач является задача поиска кратчайшего вектора решётки – именно она положена в основу криптостойкости алгоритма шифрования NTRU. Что касается теории матроидов, то она положена в основу так называемых идеальных схем разделения секрета [1].

Если говорить о *симметричной* криптографии, то следует отметить, что базовые криптографические примитивы, положенные в основу любого шифра и реализующие подстановочные и перестановочные преобразования, представляются в виде отображения $GF(2)^n \rightarrow GF(2)^m$ некоторого векторного пространства $GF(2)^n$ n-мерных двоичных векторов в другое векторное пространство $GF(2)^m$ m-мерных двоичных векторов. При этом, как замечается в [2], эффективным инструментом анализа криптографических преобразований служит математический аппарат булевых функций, в соответствии с которым каждое отображение можно представить в виде векторной булевой функции, компонентами которой являются обычные булевы функции с областью определения $GF(2)^n$ и областью значения $GF(2)$.

В отношении дисциплины «Теория информации и кодирования» следует отметить, что для её эффективного изучения требуется знание таких разделов математики, как основы теории вероятностей и теории колец и конечных полей (преимущественно полиномиальных колец и полей, т.к. именно они представляют собой удобный математический аппарат для описания одного из подклассов линейных кодов – полиномиальных циклических кодов, а также – для описания линейных сдвиговых регистров с обратными связями, находящими применение в том числе и при построении поточных алгоритмов шифрования).

Что же касается *магистерской* подготовки, то математически ёмкими в этом случае являются дисциплины «Методы анализа и построения криптосистем» и «Методы моделирования и оптимизации процессов защиты информации». Предмет изучения первой из них основан на тех же самых разделах математики, что и курс «Прикладная криптология», с той лишь возможной разницей, что в рамках этих разделов необходимо рассмотрение большего числа математических структур, положенных в основу методов криптографии и криптоанализа.

Например, для изучения *несимметричной* криптографии, основанной на идентификаторах, связанной с проблематикой электронных цифровых подписей и выступающей в качестве альтернативы подходу, известному, как PKI (Public Key Infrastructure), необходимо знание такого математического понятия, как билинейное (в общем случае – полилинейное) отображение (в этом случае преимущественно рассматривается такое бинарное отображение, как спаривание точек эллиптической кривой). Кроме того, в рамках криптоанализа билинейные отображения могут быть использованы для сведения задачи дискретного логарифмирования на эллиптических кривых к аналогичной, более простой задаче, в конечном поле.

В отношении *симметричной* криптографии, в вопросах таких видов криптоанализа, как линейный и дифференциальный криптоанализ, фундаментальную роль играет преобразование Уолша-Адамара, являющегося разновидностью дискретного преобразования Фурье [2]. Это же преобразование используется в квантовом алгоритме факторизации П. Шора.

В рамках курса «Методы моделирования и оптимизации процессов защиты информации» представляется целесообразным изучение таких тем: аналитическое и имитационное моделирование на основе аппарата теории случайных процессов (марковских и полумарковских) и систем массового обслуживания, линейная, нелинейная, комбинаторная оптимизация и булево линейное программирование, динамическое программирование, генетические алгоритмы.

Полагаем также, что для студентов, обучающимся в магистратуре, необходимо знание основ теории принятия решений в силу того, что специалистам по информационной безопасности (ИБ) регулярно приходится решать вопросы, связанные с управлением ИБ (анализ рисков ИБ, мониторинг ИБ, реагирование на инциденты и др.). Такой курс мог бы включать в себя такие разделы, как: основы теории игр, основы принятия решений в условиях неопределённости, основы построения систем поддержки принятия решений.

Что касается «чистых» математических дисциплин, входящих в план подготовки бакалавра по кибербезопасности, то, на наш взгляд, их содержание должно быть таким:

1. «Высшая математика». В основу должны быть положены разделы: линейная алгебра и её приложения, включая решение систем линейных уравнений; интегральное и дифференциальное исчисление; решение дифференциальных уравнений и их систем; числовые и функциональные ряды.

2. «Дискретная математика». Основу курса должны составлять такие классические разделы, как множества, отношения и функции; комбинаторика; графы;

основы теории алгоритмов. Представляется целесообразным в рамках основ теории множеств рассмотреть базовые положения теории нечётких множеств. В то же время, такой «классический» раздел дискретной математики, как математическая логика, было бы целесообразным, по нашему мнению, включить в качестве компонента дисциплины «Логика», другими составляющими которой могли бы быть: Аристотелева силлогистика; классическая (дедуктивная) логика (логика высказываний и логика предикатов); основы теории доказательств; некоторые неклассические логики (индуктивная (вероятностная) логика и правдоподобные рассуждения, нечёткая логика, модальная логика). В частности, о важности способности к доказательному рассуждению хорошо заметил академик В.И. Арнольд: «Роль доказательств в математике подобна роли орфографии и даже каллиграфии в поэзии. Тот, кто не научился искусству доказательства, не способен отличить правильное рассуждение от неправильного. Такими людьми легко манипулировать безответственным политикам. Результатом могут стать массовый психоз и социальные потрясения» [3]. Очевидно, что сказанное в высшей степени справедливо для специалиста в сфере информационной безопасности, особенно расширенном толковании этого понятия, когда сама информация выступает не только объектом воздействия со стороны злоумышленника, но и как средство воздействия на субъектов, что может иметь место, например, при использовании злоумышленниками методов социальной инженерии.

3. «Теория вероятностей и математическая статистика». Содержательное наполнение данной дисциплины может быть тем же, что и для тех, кто обучается по другим специальностям направления «Информационные технологии», может быть лишь с бо́льшим акцентом на изучение вопросов, связанных с проверкой статистических гипотез, что будет востребованным при изучении бакалаврской дисциплины «Прикладная криптология» (тестирование качества генераторов псевдослучайных последовательностей и анализ поточных шифров) и магистерского курса «Методы моделирования и оптимизации процессов защиты информации» (статистический анализ результатов имитационного эксперимента). Кроме того, было бы логичным в рамках данного курса рассмотреть базовые понятия теории случайных процессов в связи с последующим использованием их при изучении методов аналитического и имитационного моделирования в рамках курса «Методы моделирования и оптимизации процессов защиты информации».

Использование систем компьютерной математики в подготовке специалистов по кибербезопасности

К числу наиболее популярных систем компьютерной математики СКМ относятся Matlab, Mathematica, Maple, Mathcad. При изучении дисциплин, связанных с вопросами криптографии и криптоанализа, полезным может быть использованиев первую очередь СКМ Mathematica и Maple.

В состав этих СКМ входит пакет Number-Theory, который включает 56 и 42 функции для теоретико-числовых вычислений соответственно [4, 5].

Так, в частности, в рамках СКМ Mathematica имеется возможность генерации случайного простого числа, меньшего заданного числа n, случайного простого числа из заданного интервала чисел (например, в диапазоне $10^8 \dots 10^9$), а также списка из m случайных простых чисел в диапазоне от 2 до n; проверка числа на простоту, вычисление примитивных корней по заданному модулю, мультипликативного и обобщённого мультипликативного порядка числа по заданному модулю, вычисление теоретико-числовых функций (Эйлера, Кармайкла, Мёбиуса) и символов Лежандра и Якоби, определение мультипликативного обратного элемента и др. [5,6].

Другие популярные СКМ, такие как Mathcad и Matlab содержат лишь небольшой набор теоретико-числовых функции, а именно: *primes*, *isprime*, *factor*, *gcd*, *lcm*, *mod*. Первые три из них являются функциями одного аргумента - натурального числа n и связаны с простыми числами. Так, функция *primes* возвращает строку простых чисел, меньших или равных n, а вторая позволяет установить, является ли данное число простым. Функция *factor* решает задачу факторизации – возвращает строку, содержащую простые множители числа n. Функции *gcd* и *lcm* находят наибольший общий делитель (НОД) и наименьшее общее кратное (НОК) двух чисел соответственно и, наконец, функция *mod(x,y)* возвращает остаток от деления *x* на *y*.В то время, стоит отметить, что был разработан Number Theory Toolbox для СКМ Matlab [7], в который содержит 19 функций, позволяющих выполнять основные теоретико-числовые преобразования, встречающиеся в задачах криптографии.

С точки зрения задач прикладной криптологии в рамках СКМ Mathematica имеется возможность выполнять симметричное и несимметричное шифрование/дешифрование текстовых файлов, файлов-изображений и архивированных файлов, в том числе как и объектов облака. Несимметричное шифрование представлено криптоалгоритмомRSA, симметричное - криптоалгоритмом AES в режимах ECB и CBC. При этом пользователь может осуществлять генерацию ключей для выбранного алгоритма шифрования: 256-битового ключа для AES (случайно и на основе парольной фразы), а также генерацию ключевой пары для RSA с возможностью выбора длины модуля (в том числе и для размерности модуля 8192 бита), открытого ключа и размерности секретного ключа. СКМ Mathematica имеет встроенные функции для реализации бесключевого хеширования данных, а именно: хеш-функций MD2, MD5, SHA-1, а также

SHA-2 с размерностью дайджеста 256, 384 и 512 с возможностью представления дайджеста в шестнадцатеричной системе счисления (по умолчанию – в десятичной системе). Также СКМ Mathematica содержит встроенные функции, относящиеся к задачам частотного криптоанализа: поиск по словарю (например, отыскание всех слов на тои или ином языке, начинающихся с последовательности определённых символов, отыскание всех слов, начинающихся и заканчивающихся на интересующие исследователя символы), поиск необходимых символов (и сочетаний символов) в тексте и определение их количества, подсчёт числа всех отличных *n*-грам-последовательностей в строке символов [8,9].

Ещё одно применение СКМ – это решение задач оптимизации, рассмотрение которых, как было показано выше, предполагается в магистерском курсе «Методы моделирования и оптимизации процессов защиты информации». Анализ возможностей решения задач оптимизации в рамках СКМ Matlab, Mathematica, Maple, Mathcad сделан в работе [10].

Заключение

Содержание математических дисциплин должно определяться целями изучения математически ориентированных и других дисциплин, формирующих облик специалиста по кибербезопасности.

Математически ёмкими являются дисциплины "Прикладная криптология" и "Теория информации и кодирования" для подготовки бакалавров и курсы "Методы моделирования и оптимизации процессов" и "Методы построения и анализа криптосистем" - для магистров.

Целесообразно ввести дисциплины "Логика" и "Теория принятия решений" для магистров с целью привития будущим специалистам по информационной безопасности навыков логически выверенного системного мышления, необходимых при решении задач управления информационной безопасностью. В ходе изучения «чистых» математических и математически ориентированных дисциплин целесообразно использовать системы компьютерной математики, содержащие широкий набор встроенных функций для решения самых разнообразных задач в рамках упомянутых дисциплин.

Список литературы

1. Введение в криптографию / Под общей ред. В.В. Ященко. – СПб.: Питер, 2001. – 288 с.

2. Молдовян А.А. и др. Криптография: скоростные шифры. – СПб.: БХВ-Петербург, 2002. – 496 с.

3. Губарев В. Академик В.И. Арнольд: путешествие в хаосе // Наука и жизнь. – 2000. – №12. – с.4-10.

. Number Theoretic Functions [Электронный ресурс] // Wolfram Language & System Documentation Center – Режим доступа: http://reference.wolfram.com/language/guide/ Number Theoretic Functions.html. – 10.02.2017 г.

5. Бедратюк, Л. П. Использование системы компьютерной алгебры MAPLE в элементарной теории чисел / Л. П. Бедратюк, Г. И. Бедратюк // Восточно-Европейский журнал передовых технологий. – 2013. – №6. – С. 10–13.

6. Тилборг, ван Х.К.А. Основы криптологии. / Х.К.А. ван Тилборг. – М.: Мир, 2006. – 471 с.

7. Лысенко, И.В., Бородавка В.В. Разработка теоретико-числового тулбокса для системы компьютерной математики Matlab / И.В. Лысенко, В.В. Бородавка // Системи управління, навігації та зв'язку. – Полтава: ПНТУ ім. Ю. Кондратюка, 2017. – №2(42). – С. 89–93.

8. Cryptographic Number Theory [Электронный ресурс] // Wolfram Language & System Documentation Center, Available at: http://reference.wolfram.com/language/guide/ Cryptographic Number Theory.html - 10.05.2071.

9. Cryptography [Электронный ресурс] // Wolfram Language & System Documentation Center, Available at: http://reference.wolfram.com/language/guide/ Cryptography.html - 10.05.2017.

10. Лысенко И.В., Бутенко В.О. Анализ возможностей решения задач оптимизации средствами систем компьютерной математики [Текст] // Системи обробки інформації. – Х: ХУПС, 2016. – Вип. 5(142). – С. 133–136.

Надійшла до редколегії 21.08.2017

Рецензент: д-р техн. наук, проф. В.С. Харченко, Національний аерокосмічний університет ім. М.Є. Жуковського «ХАІ», Харків.

.

ПРО МАТЕМАТИЧНУПІДГОТОВКУ СТУДЕНТІВ, ЯКІ НАВЧАЮТЬСЯ ІЗ СПЕЦІАЛЬНОСТІ «КІБЕРБЕЗПЕКА»

І.В. Лисенко

Сформульовано пропозиції рекомендації щодо змісту і викладання математичних і математично орієнтованих дисциплін студентам, які навчаються з спеціальності «Кібербезпека». Розглянуто розділи математики, необхідні для вивчення дисциплін, що формують випускника-бакалавра або магістра в галузі інформаційної безпеки. Обґрунтовано доцільність використання систем комп'ютерної математики в процесі вивчення математично орієнтованих дисциплін

Ключеві слова: *кібербезпека, криптологія, системи комп'ютерної математики.*

ABOUT MATHEMATICAL TRAINING OF THE STUDENTS WHO LEARN ACORDING TO THE SPECIALTY "CIBERSECURITY"

I.V. Lysenko

Propositions and recommendations relatively content and teaching of the mathematic and mathematic oriented disciplines for students training on specialty "Cybersecurity" are formulated. The mathematics chapters necessary for studying of the disciplines that form of the bachelors and masters in the sphere of information security are considered. Advisability of using of the systems of computer mathematics during studying of the mathematic oriented disciplines are justified.

Keywords: *cybersecurity, cryptology, systems of computer mathematics.*