УДК 373.1+377.1
ББК 74.262.21+74.47

DOI: 10.31862/1819-463X-2020-1-139-153

ТЕОРИЯ И ПРАКТИКА ОБУЧЕНИЯ ШКОЛЬНИКОВ И СТУДЕНТОВ СПО ОСНОВАМ ЗАЩИТЫ ИНФОРМАЦИИ

Е. И. Деза, Л. В. Котова, Е. С. Лебедева

Аннотация. *В статье рассмотрены теоретические основы, методические возможности и практические проблемы обучения школьников 10–11-х классов и студентов среднего профессионального образования основам защиты информации. Проанализирована роль защиты информации в современном цифровом обществе. Доказана необходимость знакомства с базовыми вопросами защиты информации школьников и студентов. Раскрыто место дисциплины «Криптография» в системе современного отечественного общего и профессионального образования. Обоснована методическая целесообразность разработки и внедрения в педагогическую практику курса «Криптография для всех», предназначенного для знакомства с основами защиты информации старшеклассников и студентов среднего профессионального образования, обучающихся по «непрофильным» специальностям. На основе выделения особенностей криптографии как области научного знания сформулированы вопросы практической реализации такого курса и методические характеристики его учебно-методического обеспечения. Выделены принципы создания учебного пособия «Криптография для всех». Уточнены критерии отбора его математического содержания. Перечислены дидактические функции данного пособия. Разработаны требования к его структуре. Представлено подробное описание структуры пособия. Рассмотрены вопросы практической реализации разработанных материалов.*

Ключевые слова: *защита информации, криптография, метапредметность, доступность, прикладная направленность, универсальность знаний, исследовательская деятельность обучающихся.*

THEORY AND PRACTICE OF TEACHING SCHOOL AND UNIVERSITY STUDENTS THE BASICS OF INFORMATION SECURITY

E. I. Deza, L. V. Kotova, E. S. Lebedeva

Abstract. *The article considers the theoretical foundations, methodological capabilities and practical problems of teaching schoolchildren and students of secondary vocational*

education the basics of information security. The role of information security in a modern digital society is analyzed. The necessity of introducing the basic issues of protecting information of schoolchildren and students is proved. The place of the discipline „Cryptography" in the system of modern domestic general and professional education is disclosed. The methodological feasibility of developing and introducing into the pedagogical practice the course "Cryptography for All", designed to introduce the basics of protecting information of high school students and students of secondary vocational education, students in "non-core" specialties, is substantiated. Based on highlighting the features of cryptography as an area of scientific knowledge, the questions of the practical implementation of such a course and the methodological characteristics of its educational and methodological support are formulated. The principles of creating the textbook „Cryptography for All" are highlighted. The selection criteria for its mathematical content have been clarified. The didactic functions of this manual are listed. Requirements for its structure are developed. A detailed description of the structure of the manual is provided. Issues of practical implementation of the developed materials are considered.

Keywords: *information security, cryptography, meta-subject, availability, applied orientation, pansophy, research activities of students.*

Информационное общество и образование. Сегодня требования, предъявляемые к отечественной образовательной системе, как никогда высоки, а цели, стоящие перед современным образованием, грандиозны. Если говорить коротко, основной образовательной парадигмой постиндустриального цифрового общества является подготовка человека новой формации, приспособленного к реалиям этого общества, то есть индивида мобильного, широко эрудированного, хорошо ориентирующегося в безумном по объемам и скоростям информационном потоке, великолепно владеющего современными методами и средствами поиска, передачи, переработки, хранения и непрерывной корректировки информации. Сегодня все мы подвешены на информационных ресурсах и средствах их использования, как марионетки на нитях. Можно обсуждать плюсы и минусы сложившейся ситуации, но реалии сегодняшнего дня именно таковы. Необходимо так или иначе приспосабливаться к ним на всех уровнях, в том числе на уровне организации образовательного процесса современной школы.

Защита информации – актуальная проблема современного общества. Если речь идет об информации, то невозможно оставить без внимания и вопросы ее защиты. Несмотря на регулярное использование в повседневной жизни тех или иных схем информационной защиты, мы до сих пор остаемся потрясающе безграмотными в этой области. Знакомство молодого поколения с основами защиты информации – и на практических примерах, и путем демонстрации математических оснований этой области знаний – насущная проблема современного образования на всех его уровнях.

Место криптографии в современном образовании. Хотя глобальное решение этой проблемы – вопрос будущего, следует отметить, что ряд наработок в этой области, на которые можно опереться, уже имеется. Вопросам защиты информации посвящено сегодня немало учебников, учебных пособий, другой литературы, как глубокого профессионального толка (О. Н. Василенко [1], А. Ю. Нестеренко [2], Н. Коблиц [3], Б. Я. Рябко и А. Н. Фионов [4], Б. Шнайер [5] и др.), так и популярного уровня, дающих представления о современных задачах криптографии в виде, доступном даже учащимся общеобразовательной школы (У. Болл и Г. Коксетер [6], В. В. Ященко и др. [7], М. Гарднер [8], Ж. Гомес [9], С. Я. Дориченко и В. В. Ященко [10] и др.).

За последние годы в программах большого числа направлений подготовки высшего образования (далее – ВО) появилась дисциплина «Основы защиты информации» (или родственные ей дисциплины «Основы криптографии», «Методы и средства защиты информации» и др. – см., например, [11]). Аналогичные дисциплины можно найти и в программах ряда специальностей среднего профессионального образования (далее – СПО) (см., например, [12]).

В общеобразовательной школе вопросы защиты информации затрагиваются в современном курсе информатики только углубленного уровня. Так, например, в учебно-методическом комплексе «Информатика» для 10–11-х классов И. А. Калинина и Н. Н. Самылкиной [13] можно найти раздел «Система RSA, ключи открытые, закрытые, их получение». В базовых курсах информатики основы криптографии освещаются достаточно слабо (так, в учебнике Л. Л. Босовой и А. Ю. Босовой «Информатика» для 5-го класса [14] рассмотрена тема «Шифры»; в учебнике Н. Д. Угриновича «Информатика» для 10–11-х классов [15] представлен раздел «Компьютерные вирусы и защита от них»; в учебнике Н. В. Макаровой «Информатика» для 10–11-х классов [16] проанализированы организационные меры информационной безопасности – речь идет об антивирусах), и познакомиться с ними учащиеся могут только в рамках олимпиад по криптографии, а также в ходе единичных междисциплинарных курсов по выбору соответствующей тематики.

Следует отметить, что на уровне высшего образования большая работа по внедрению соответствующих дисциплин в образовательный процесс уже дает свои плоды. Разработаны, апробированы и внедрены в образовательный процесс учебно-методические комплексы (УМК), включающие программы курсов, учебные и учебно-методические пособия, электронные курсы (см. [17–19] и др.). Появился ряд научно-методических исследований, освещающих различные аспекты указанной проблематики.

В системе СПО на сегодняшний день сложилась несколько иная ситуация. С одной стороны, курсов, так или иначе рассматривающих вопросы защиты информации, становится все больше, разрабатываются программы, авторы которых стараются максимально охватить все стороны проблематики, однако зачастую эти программы выполнены на достаточно низком математическом уровне. С другой стороны, дисциплины, так или иначе рассматривающие вопросы защиты информации, представлены далеко не для всех специальностей. Так, в программах специальностей СПО 21.02.05 Земельно-имущественные отношения и 40.02.30 Право и судебное администрирование, реализуемых в Российском государственном университете правосудия, соответствующая дисциплина не предусмотрена. Общие слова о защите информации можно найти для указанных специальностей в рабочих программах дисциплин «Информатика», «Основы безопасности жизнедеятельности», профессионального модуля «Информатизация деятельности суда» (охватывающего несколько дисциплин специальности 40.02.03), но этому уделяется очень мало времени. Про кодирование информации упоминается только в курсе информатики, причем акцент сделан лишь на алгоритмы перевода чисел из одной системы счисления в другую. При этом нет сомнений в том, что для работников юридических специальностей знание основ защиты информации, понимание принципов работы соответствующих механизмов жизненно необходимо (огромный документооборот, работа с сайтами судов и т. д.). Кроме того, преподаватели сталкиваются с объективными трудностями внедрения в практику уже имеющихся разработок: в силу своего возраста и уровня предварительной подготовки обучающиеся далеко не всегда готовы к усвоению предлагаемого им объема информации. Наконец, в системе СПО практически нет соответствующих учебно-методических материалов, в частности, отсутствуют учебные пособия, предназначенные для знакомства обучающихся СПО с основами криптографии. Сегодня такая ситуация просто недопустима.

Что касается общеобразовательной школы – знакомство учащихся с математическими основами защиты информации отдано сегодня на откуп энтузиастам, которые, проводя огромную работу в отдельно взятом образовательном учреждении, в рамках того или иного единичного конкурсного мероприятия, не ставят перед собой задачу построения единого систематического курса, доступного и необходимого всем учащимся. Уклон соответствующей подготовки очень конкретен: прежде всего – олимпиадный, несколько шире – занимательный. Содержание, соответственно, очень «симпатично», включает в себя множество интересных фактов и задач, но подпадает под определение «с бора по сосенке». Предлагаемые задачи не образуют системы, не имеют специально разработанной единой математической базы.

Можно утверждать, что проблема создания систематических курсов по криптографии для ВО частично решена. Такие дисциплины разработаны, для них созданы пособия и электронные курсы. В качестве примера можно привести учебное пособие Е. И. Деза и Л. В. Котовой «Теоретико-числовые основы защиты информации», предназначенное для студентов математических факультетов педагогических вузов [19]. Однако как упомянутое выше пособие, так и соответствующий ему курс предназначены для студентов, профессионально ориентированных на использование вопросов защиты информации. Думаем, что его же можно адаптировать и для «профильного» СПО (то есть для соответствующих специальностей СПО), добавив те или иные блоки информации, в зависимости от конкретной ситуации.

К сожалению, этого нельзя сказать об общеобразовательной школе и системе «непрофильного» СПО. На наш взгляд, назрела необходимость создания единого курса по криптографии, предназначенного для указанной аудитории. Курса для «неспециалистов» в области защиты информации, нуждающихся в нем как по общим причинам, указанным выше (формирование основ информационной грамотности в реалиях современного информационного пространства, окружающего нас), так и для профессиональной ориентации (школа) или «профессионального взгляда» на вопрос (студенты СПО).

Особенности криптографии как области научного знания. Прежде чем переходить к обсуждению проблем построения такого курса, попробуем ответить на вопрос: почему именно криптография призвана стать его содержательной основой? Основное мы уже сказали: живя в информационном обществе, невозможно обойтись без знания базовых положений об информации как общекультурном феномене, в том числе без сформированного представления о современных способах ее защиты (которые мы уже давно используем, пусть неосознанно, в повседневной жизни). Другими словами, криптографию прежде всего затем изучать надо, что она завязана – и многопланово – на цифровые технологии, которые сегодня являются неотъемлемой составной частью нашей жизни.

Это, конечно, главное, но не все. Криптография – наука очень интересная со многих точек зрения. Среди ее *отличительных особенностей* можно выделить широкие возможности криптографии как самостоятельной ветви знаний, объединяющей целый ряд различных дисциплин, в том числе математику, информатику, физику, экономику (не забудем и тесные связи с историей, литературой, географией и другими науками), определяющие ее *метапредметность*. В свою очередь, метапредметность, требуя, с одной стороны, *фундаментальности* в изложении основ, с другой стороны, позволяет включать в изложение целый спектр вопросов из различных областей знаний, понятных каждому, что реализует *прикладную направленность* предлагаемых материалов, одновременно обеспечивая их *доступность*. При этом появляется возможность сделать акцент на развивающую и познавательную составляющие содержания, в силу чего у обучающихся формируется *мотивация на исследовательскую деятельность*, на получение новых знаний, на поиск новых областей исследования.

Такое уникальное сочетание особенностей анализируемой области знаний позволяет, при грамотном подходе, решить ряд важных дидактических задач. А именно можно считать, что *универсальность* является основным, глобальным свойством дисциплины «Криптография» и соответствующей области научного знания. В этом случае правильная организация учебного процесса позволит нам при обучении криптографии способствовать формированию *универсальности знаний* учащихся и студентов, решая тем самым одну из актуальнейших задач модернизации отечественного образования [20]. На наш взгляд, систематическое обучение криптографии в рамках междисциплинарного курса для школьников (или студентов СПО) позволит реализовать следующую формулу (рис.).

В этом контексте *универсальность* формируемой у обучающихся системы знаний и *готовность* школьников и студентов *к самостоятельной исследовательской деятельности* представляют собой основную *цель* соответствующей дидактической модели, в то время как *метапредметность, прикладная направленность, доступность* и *фундаментальность* в комплексе представляют собой *средство (рецепт) достижения, реализации* указанной цели.

Следует добавить, что в сложившихся обстоятельствах представленная выше формула будет нежизнеспособной без *методической* составляющей: реализовать предложенную дидактическую модель может только специалист, полностью владеющий соответствующей методикой и обеспечивающий профессиональное сопровождение обучающихся на всех этапах освоения дисциплины.

«Непрофильный» курс криптографии: вопросы реализации. Опираясь на вышесказанное, можно утверждать, что любой «непрофильный» курс криптографии должен быть направлен на обеспечение *универсальности* знаний обучающихся и *формирование* их *готовности к исследовательской деятельности* на основе использования *метапредметности* (рассматриваем максимально широкий спектр вопросов из разных областей знания), *прикладной направленности* (демонстрируем важные *прикладные, практико-ориентированные и популярные задачи*, максимально приближенные к реалиям повседневной жизни), *доступности* (при выборе материала делаем упор на *задачи, которые несложно понять и усвоить* даже со скромной математической базой). При этом курс должен быть систематическим, представлять собой единую, логически построенную завершенную (но при этом модульную) дисциплину, опирающуюся на *фундаментальность* изложения ее математических основ.

Помогая обучающимся развивать свой когнитивный потенциал, формируя их готовность к самостоятельной исследовательской деятельности, адаптируя их к реалиям современного цифрового общества, освещая с новой точки зрения ряд явлений и фактов повседневной жизни, мы не должны забывать и о профессиональной составляющей обучения. При освоении курса криптографии это сделать нетрудно. Для школьников профессиональная ориентация реализуется, прежде всего, за счет на-

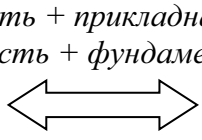

Рис. Формула соответствия целей и средств их достижения при обучении криптографии

личия большого спектра задач из различных областей знаний, большинство из которых предоставляют учащемуся возможность более глубоко ознакомиться с предметом, в том числе в рамках индивидуальной проектной деятельности. Для студентов СПО профессиональная ориентация (точнее, «профессиональный взгляд» на проблематику) – это наличие задач, тесно связанных с соответствующей специальностью: мы рассматриваем те вопросы, которые нужны и важны в будущей профессиональной деятельности именно этих студентов. Благодаря особенностям криптографии, обычно подбор таких задач не представляет труда.

«Непрофильный» курс криптографии: учебно-методическое обеспечение. Создание нового курса – дело долгое и сложное. Прежде всего, нужно разработать собственно курс – систематический, целостный, построенный в рамках единой концепции и базирующийся на четких теоретических основаниях (принципы создания, критерии отбора содержания и др.). Дальнейшая работа связана с разработкой учебного пособия, соответствующего разработанному курсу, выполняющего выделенные специфические функции и отвечающего ряду специальных требований. В дальнейшем эта работа может привести к созданию соответствующего электронного курса, дополнительных дидактических материалов и т. д.

Чем бы мы ни занимались, начать придется с подбора и систематизации имеющихся материалов. Как уже было сказано, вопросам защиты информации посвящено немало работ, как профессиональных [1–5], так и популярных [6–10]. Особенно полезными, с нашей точки зрения, являются книги В. В. Ященко, О. Н. Василенко, А. Ю. Нестеренко. Интересны сборники олимпиадных задач по криптографии. Много полезного материала можно найти в уже упомянутом выше пособии Е. И. Деза и Л. В. Котовой [19]. Однако разброс материалов слишком велик. В сборниках олимпиадных и развивающих задач представлено много заданий, но нет достаточной систематизации по подходам к их решению, да и сами подходы слишком отличаются, от подбора ответа до серьезной аналитическо-математической работы; популярная литература зачастую не содержит практических заданий, позволяющих не только познакомиться с материалом, но и освоить его практическую сторону; сложная научная литература, как правило, имеет уровень изложения материала заведомо более высокий, чем у школьников и студентов СПО.

Другими словами, сегодня явно не хватает учебных и учебно-методических пособий, в полной мере учитывающих *метапредметность* дисциплины, сочетающих *популярную* (познакомить), *фундаментальную* (дать математические основы и закрепить) и *прикладную* (показать приложения) составляющие, обеспечивающих *доступность* изложения и опирающихся на серьезное *методическое сопровождение*.

При разработке «непрофильного» курса криптографии для старшеклассников и студентов СПО мы рассматривали создание такого пособия как первостепенную задачу: будет пособие – состоится и курс. В ходе работы мы пытались учесть все перечисленные выше аспекты, дополнительно помня о необходимости обеспечить материалами целый систематический курс; построить цикл взаимосвязанных, но самодостаточных (сменный контингент слушателей) занятий; организовать проектную деятельность с группой или отдельным учеником.

Для реализации всех планов мы использовали ряд теоретических подходов и практических приемов, большинство из которых представлены ниже.

Принципы разработки учебного пособия «Криптография для всех». Процесс создания учебно-методического обеспечения «непрофильного» курса криптографии для школьников и студентов СПО будет более эффективен, если при его реализации опираться на следующие *принципы: системности и целостности; метапредметности и интегративности; популярности и доступности; прикладной направленности; универсальности и фундамен-*

тальности; ориентации на исследовательскую деятельность; гуманизации и личностной детерминации; ИКТ-поддержки; гибкости и обоснованности инноваций; непрерывности и преемственности; модульной самодостаточности и распределенности; вариативности; профессиональной ориентации [21–24].

Принцип системности и целостности означает, что разработанный курс должен представлять собой единую, законченную систему функционально взаимосвязанных структурных компонентов, объединенных единой образовательной целью. *Принцип метапредметности и интегративности* требует максимально использовать метапредметный характер курса, его интегративные, межпредметные составляющие, инвариантные связи и отношения, способствующие целостному видению изучаемых проблем во всей их полноте, многогранности и многоаспектности. *Принцип популярности и доступности* ориентирует нас на использование материалов, максимально приближенных к реалиям повседневной жизни, понятных каждому, позволяющих на конкретных примерах ввести обучающегося в предмет и, наоборот, продемонстрировать известные жизненные ситуации с точки зрения современной науки. *Принцип прикладной направленности* обеспечивает знакомство обучающихся с максимально широким спектром применений вопросов защиты информации в различных областях знаний. *Принцип универсальности и фундаментальности* подразумевает, что дисциплина должна обеспечивать универсальность знаний обучающихся без потери фундаментальности этих знаний, что математическое содержание разрабатываемого курса должно отражать фундаментальные основы соответствующей математической теории, охватывать все базовые утверждения и идеи данного раздела математической науки. *Принцип ориентации на исследовательскую деятельность* напоминает о том, что одной из основных задач курса является формирование готовности обучающихся к самостоятельной учебно-исследовательской и проектной деятельности. *Принцип гуманизации и личностной детерминации* предусматривает наличие средств формирования индивидуального маршрута прохождения курса, максимально отвечающего личностной ориентации каждого, его индивидуальным предпочтениям, способностям и возможностям. *Принцип ИКТ-поддержки* означает, что дисциплина тесно и многопланово связана с современными цифровыми технологиями и ее освоение невозможно без существенного использования в образовательном процессе средств ИКТ. *Принцип гибкости и обоснованности инноваций* предполагает при разработке новых средств обучения максимальное сохранение имеющегося опыта, бережного отношения к содержанию классических математических курсов, отточенному десятилетиями творческой работы многих поколений преподавателей. *Принцип непрерывности и преемственности* требует учитывать, что подготовка в рамках курса представляет собой часть непрерывного процесса формирования человека нового общества, поэтапно осуществляемого в рамках школьного, среднего профессионального и вузовского образования и реализующего идею образования «через всю жизнь». *Принцип модульной самодостаточности и распределенности* подразумевает организацию изучения дисциплины, при которой ориентация на последовательную реализацию всех этапов обучения, оптимальное обоснованное распределение содержания курса, методов и форм его освоения в соответствии с основными этапами обучения естественным образом сочетается с содержательной, смысловой и организационной законченностью каждого отдельного этапа (модуля). *Принцип вариативности* подразумевает предоставление обучающемуся возможности индивидуализированного овладения дисциплиной на основе выделения инвариантной и вариативной составляющих ее содержания. *Принцип профессиональной ориентации* предполагает, что содержательные и дидактические составляющие курса должны быть согласованы с нуждами профессионального опреде-

ления школьников и вопросами приобретаемой профессии студентов СПО.

Критерии отбора математического содержания учебного пособия «Криптография для всех». Отбор математического содержания учебного пособия, направленного на поддержку нашего курса, должен в этих условиях соотноситься с *критериями содержательного единства и системности, непрерывности и преемственности, научности и фундаментальности, многоплановости и веерности, популярности и доступности, прикладной направленности, актуальности и перспективности, соответствия возрастным и индивидуальным особенностям обучающихся, профессиональной ориентации и профессиональной значимости, соответствия учебно-методическому и технологическому обеспечению, соответствия учебному времени* [21].

В нашем контексте *критерий содержательного единства и системности*, равно как и *критерий непрерывности и преемственности*, отражает направленность на создание единого систематического курса по криптографии, предназначенного для указанной выше целевой аудитории. *Критерий научности и фундаментальности* подчеркивает, что разрабатываемый курс, несмотря на все его особенности, базируется на едином математическом фундаменте, прочной логически завершенной теоретической базе. *Критерии многоплановости и веерности, популярности и доступности, прикладной направленности* с разных сторон освещают особенности курса, связанные с его метапредметностью: как можно более широкий, веерный охват понятных и доступных примеров из повседневной жизни, других областей знаний, прикладных областей. *Критерий актуальности и перспективности*, помимо других аспектов, учитывает ориентацию курса на организацию исследовательской работы обучающихся, в то время как *критерий соответствия возрастным и индивидуальным особенностям* обучающихся, кроме того, напоминает нам, что наша целевая аудитория имеет определенный возрастной лимит, который необходимо учитывать в ходе отбора содержания курса. Наконец, говоря о *критерии соответствия технологическому обеспечению*, не будем забывать о том, что и технологическое обеспечение должно соответствовать решаемым задачам – без хорошей ИКТ-базы грамотная реализация курса невозможна.

Функции учебного пособия «Криптография для всех». В этих условиях классические *обучающую, воспитывающую* и *развивающую* функции учебных пособий следует детализировать, выделив следующие *функции* разрабатываемого нами учебного пособия [21; 22]:

- *информационная* – передача основной и дополнительной информации, в том числе популярных, жизненных примеров из области защиты информации, математических основ курса, прикладных аспектов дисциплины, исследовательских проблем;
- *систематизирующая* – структуризация и систематизация содержания, демонстрация содержательно-смысловой и логической схемы дисциплины;
- *диверсификационная* – реализация метапредметных свойств дисциплины, обеспечение многоплановости предлагаемых задач и дополнительной информации, широкого разброса, веерности предлагаемых материалов из различных областей знаний;
- *адаптационная* – обеспечение системы знаний в широком спектре практико-ориентированных ситуаций, связанных с защитой информации;
- *интеграционная* – демонстрация содержательного единства метапредметной дисциплины, создание внутренних и внешних информационных связей, формирование универсальной системы знаний на базе выделения инвариантных составляющих содержания;
- *навигационная* – обеспечение поиска дополнительной информации на основе имеющегося списка литературы и других дополнительных источников, в том числе при реализации исследовательской и проектной деятельности;
- *мотивационная* – повышение интереса к дисциплине, побуждение к учебно-

познавательной, в частности, исследовательской и проектной, деятельности;

● *рефлексивная* – обеспечение адекватной самооценки обучающегося как при освоении дисциплины, так и в ситуациях повседневной жизни, связанных с вопросами защиты информации;

● *коррекционная* – возможность выбора и своевременной коррекции как индивидуального маршрута освоения дисциплины, так и методов и способов использования современных средств защиты информации в повседневной жизни;

● *профориентационная* – обеспечение задач, демонстрирующих вопросы защиты информации в самом широком спектре областей знаний и жизни (школьник) или в вобранной профессиональной области (студент СПО);

● *методическая* – обеспечение непрерывной поддержки и руководства процессом изучения дисциплины, эффективного мониторинга промежуточных результатов обучения, объективной итоговой комплексной оценки.

Требования к структуре учебного пособия «Криптография для всех». В связи с существенным расширением выполняемых функций возникают и дополнительные *требования к структуре пособия* [23; 24]:

● *единство структуры и содержания*; все разделы пособия должны быть изложены по одной схеме, с жестким соблюдением логической последовательности математического построения курса, строгости и достаточной полноты подачи материала;

● *оптимальное сочетание строгости* изложения *и доступности* материалов; строгость изложения не должна сопровождаться перегруженностью формальными математическими выкладками, математические основы должны сопровождаться необходимыми комментариями и примерами;

● *изложение* основного материала *в виде конструктивно выделенных модулей*, взаимодополняющих, но содержательно самостоятельных; как правило, такие модули соответствуют тем или иным разделам пособия;

● *наличие явно выделенных блоков*, *содержащих вспомогательную, дополнительную и справочную информацию*; они могут быть представлены мелким шрифтом, выделены в комментарии и т. д.;

● *снабжение текста пособия перекрестными ссылками*, которые реализуют «внутренние» связи содержания, выполняют роль интегративного остова, обеспечивающего системность конструкции;

● *наличие ссылок на другие учебники и учебные пособия*, научно-популярную литературу, интернет-сайты и другие источники информации не только по предмету, но и из смежных областей знаний, что обеспечивает «внешние» связи содержания; заметки для учителя о дополнительных ресурсах, с указанием приложений, полезных для организации исследовательской деятельности обучающихся;

● *содержательное и структурное обеспечение многоплановости и веерности предлагаемых задач*; наличие примеров из реальной жизни и заданий практической направленности, обеспечивающих популярность и доступность материала;

● *наличие широкого спектра прикладных задач* из разных областей знаний, в том числе профессионально-ориентированных;

● *обязательное наличие* популярно изложенных *исторических и естественнонаучных аспектов*;

● *наличие списка исследовательских задач*, творческих заданий на основе материалов каждого модуля, в функции которых входит обеспечение индивидуальной и групповой проектно-исследовательской деятельности обучающихся;

● *включение в текст занимательных задач*, в том числе задач из школьных учебников, задач олимпиадного типа и др.;

● *включение в текст серии примеров*, как можно шире демонстрирующих различные подходы к работе с материалом;

● *наличие заданий для (само)проверки и (само)контроля*, в том числе примерных вариантов самостоятельных и контрольных работ, примеров олимпиадных задач изучаемой тематики;

● *обеспечение возможности информационно-коммуникационной поддержки* усвоения материала: выполнение заданий с использованием вычислительной техники; другие возможности оптимизации обучения на базе ИКТ.

Описание структуры учебного пособия «Криптография для всех». Как было сказано выше, пособие «Криптография для всех» предназначено для школьников 10-11-х классов и студентов СПО «непрофильных» направлений подготовки. Оно состоит из четырех разделов. Каждый раздел имеет одну и ту же структуру: популярные вопросы, математические основы темы, примеры, практика, проекты.

Рассмотрим содержание каждого раздела более подробно.

История секретов. История, литература, искусство и криптография. Терминология. Математические основы – простейшие задачи с описанием различных методов

Таблица

Структура учебного пособия «Криптография для всех»

Блок	Описание	Примеры
1. История секретов		
Популярное	*В истории* (военное искусство, стеганография)	Скитала, диск Энея, шифр аббата Тритемиуса и др.
	В литературе	А. Конан-Дойл «Пляшущие человечки», Э. По «Золотой жук»
	В обществе	Тюремная азбука, решетки Кардано в светских альбомах
Теоретические основы	*Терминология*: шифр, основные параметры: ключ, шифрование-кодирование, дешифрование. *Критерий* однозначности, *классификация* шифров	Шифры простой замены, полиалфавитные шифры, перестановки
	***Математика*: начала теории сравнений; аффинные преобразования**	***Вычисления по модулю, примеры аффинных преобразований**
Задачи	*Ознакомительные* : в задаче описан метод – следует зашифровать, прочесть	«Уголки», «Тарабарская грамота», «Парный шифр», «Шифр по книге»
	Практические	***Аффинные криптосистемы и их параметры**
Творческие (проектные) работы	*Межпредметные исследования.* Творческие работы на исследование различных классов и видов шифрования	«Такие разные решетки Кардано» (литература, искусство, математика, история). «Перестановки. Так ли их много?» (математика, информатика, история). «Создаем собственные шифры и коды» (математика, история, информатика, юриспруденция). «Криптография в современной художественной литературе» (литература, математика, информатика, история)
Литература.	*Самая широкая* – историческая и популярная	См.: [7; 8; 10; 14]

Продолжение таблицы

Блок	Описание	Примеры
2. Искусство взлома чужих секретов		
Популярное	*История вскрытия отдельных шифров*. Метод частотного анализа (XV в.). Д. Валлис, первая криптографическая служба	Вскрытие скиталы, линейки Энея, текстов с простой заменой
Теоретические основы	*Терминология*: криптография, криптоанализ, криптостойкость, частотный анализ. *Метод Казисского, принцип Керкгоффса*	Количество ключей. Применение частотного анализа к вскрытию сообщений
	*** *Математика*: аффинные преобразования и их криптоанализ (решение сравнений)**	***Примеры вскрытия аффинных преобразований**
Задачи	*Демонстрационные*: комбинаторные; перебор и анализ (частотный анализ)	Какой сейф надежнее? Вскрытие текстов с применением частотного анализа
	Практические	***Криптоанализ аффинных криптосистем**
Творческие (проектные) работы	*Межпредметные исследования* по математике и информатике	«Вскрываем, привлекая возможности компьютера». «Разрабатываем свои криптосистемы»
Лит-ра	*Научно-популярная*	См.: [3; 4; 5; 19]
3. Олимпиадные задачи по криптографии		
Популярное	*История олимпиад*	Примеры простых задач
Теоретические основы	*Математические основы:* комбинаторные формулы, свойства сравнений (теория остатков)	Примеры решения базовых задач
Задачи	*Задачи олимпиад по криптографии*	Разбор решений задач разного типа
Творческие (проектные) работы	*Анализ и конструирование заданий олимпиад* (математика)	«Составляем олимпиадные задачи». «Решаем задачи олимпиад различными способами»
Лит-ра	*Школьная, олимпиадная*	См.: [7; 10; 11; 19]
4. Криптография сегодня		
Популярное	*Коды в быту*: штрихкоды, банковские карты, электронная подпись	Примеры вычисления контрольной цифры штрихкода и банковской карты

Окончание таблицы

Теоретические основы	*Работа в EXCEL.* *Формулы* вычисления контрольной цифры штрихкода и кредитной карты. Обратные вычисления	Реализация простейших программ в *EXCEL.* Примеры вычислений контрольных цифр
	*** *Математика*: функция Эйлера, математическое описание работы RSA, электронной подписи**	***Генерирование ключей. Пример реализации передачи сообщения с открытым ключом, с электронной подписью**
Задачи.	*Составление и реализация программ в EXCEL*	Восстановление стертой цифры штрихкода
	Практические	***Генерирование ключей**
Творческие (проектные) работы	Исследования математических, социальных, юридических и других аспектов современных криптосистем	«Как найти стертую цифру в штрихкоде?» (математика, информатика). «Юридические основы использования современных криптосистем». (юриспруденция, информатика). «Что такое криптографический ГОСТ? Зачем он нужен?» (информатика, юриспруденция, экономика). «Атаки и защита от них» (информатика, юриспруденция, математика)
Литература	*Самая широкая* – математическая, учебная, юридическая, экономическая, научно-публицистическая, популярная	См.: [1–19]

шифрования. Исторические задачи шифрования. Творческие (проектные) межпредметные работы на анализ старинных шифров и создание собственных, исследование освещения криптографии в современной художественной литературе.

Искусство взлома чужих секретов. История, литература, искусство – примеры вскрытия простейших шифров. Классификация методов. Принцип Керкгоффса. Простейшие задачи на вскрытие. Решение задач на криптоанализ. Творческие работы на анализ различных методов криптоанализа и комбинирование методов шифрования.

Олимпиадные задачи по криптографии. История, математика, комбинаторика, начала теории сравнений. Олимпиадные задачи. Задачи «на составление задач». Различные решения одной задачи.

Криптография сегодня. Повседневность: штрихкоды, банковские карты, работа в *EXCEL*. Глобальная защита информации: математика, информатика, экономика, физика, юриспруденция. Теория сравнений: примеры задач; решение задач. Программирование и работа с приложениями.

Детальный анализ структуры каждого из разделов приведен в таблице. Жирным шрифтом выделены математические вопросы, объем которых можно «дозировать» в зависимости от конкретной аудитории.

Выводы. Опыт практической работы авторов в Институте математики и информатики Московского педагогического государственного университета, на кафедре общеобразовательных дисциплин Российского государственного университета правосудия, в общеобразовательных школах города Москвы, в Московском центре непрерывного математического образования позволяет утверждать, что учебное пособие «Криптография для всех», предназначенное для поддержки «непрофильного» курса криптографии для старшеклассников

и студентов СПО, востребовано современной отечественной образовательной системой. Внедрение в учебный процесс материалов, представляющих собой составные части представленного в статье учебного пособия, способствует решению актуальных задач, связанных с заявленной тематикой. Среди них: знакомство молодежи с современными методами защиты информации в рамках практических и теоретических аспектов этой области знаний, формирование универсальности знаний обучающихся, их готовности к самостоятельной исследовательской деятельности. Кроме того, можно говорить о повышении общей и математической культуры школьников и студентов, усилении их мотивации к познавательной деятельности, адаптации к реалиям современного цифрового общества. Все вышесказанное позволяет судить о целесообразности применения разработанного пособия в междисциплинарной подготовке школьников и студентов СПО и свидетельствует об эффективности использования его особенностей для повышения качества такой подготовки.

СПИСОК ЛИТЕРАТУРЫ

1. *Василенко О. Н.* Теоретико-числовые алгоритмы в криптографии. М.: МЦНМО, 2003. 328 с.
2. *Нестеренко А. Ю.* Теоретико-числовые алгоритмы в криптографии. М.: МГИЭиМ, 2012. 224 с.
3. *Коблиц Н.* Курс теории чисел и криптографии. М.: Научное изд-во ТВП, 2001. 260 с.
4. *Рябко Б. Я., Фионов А. Н.* Основы современной криптографии и стеганографии. М.: Горячая линия-Телеком, 2011. 232 с.
5. *Шнайер Б.* Прикладная криптография. М.: Триумф, 2002. 816 с.
6. *Болл У., Коксетер Г.* Математические эссе и развлечения. М.: Мир, 1986. 472 с.
7. Введение в криптографию / под общ. ред. В. В. Ященко. М.: МЦНМО, 2012. 348 с.
8. *Гарднер М.* От мозаик Пенроуза к надежным шифрам. М.: Мир, 1993. 416 с.
9. *Гомес Ж.* Мир математики. Математики, шпионы и хакеры. Кодирование и криптография. М.: Де Агостини, 2014. 144 с.
10. *Дориченко С. Я., Ященко В. В.* 25 этюдов о шифрах. М.: ТЕИС, 1994. 69 с.
11. *Котова Л. В.* Рабочая программа дисциплины «Методы и средства защиты информации». Направление подготовки: 050100.62 Педагогическое образование. Профиль подготовки: Информатика. М.: МПГУ, 2012. 24 с.
12. *Гринько Д. И.* Программа междисциплинарного курса ДК.02.01. Криптографическая защита информации. URL: http://www.informio.ru/fond/2677/Programma-mezhdisciplinarnogo-kursa-MDK0201-Kriptograficheskaja-zashita-informacii (дата обращения: 30.07.2019).
13. *Калинин И. А., Самылкина Н. Н.* УМК «Информатика», 10–11 классы. Углубленный уровень. М.: Бином, 2014. 344 с.
14. *Босова Л. Л., Босова А. Ю.* Информатика: учебник для 5 класса. М.: Бином, 2015. 184 с.
15. *Угринович Н. Д.* Информатика. Учебник для 10–11 кл. М.: Лаборатория Базовых Знаний, 2011. 512 с.
16. *Макарова Н. В.* Информатика. 10–11 класс. СПб.: ПитерКом, 1999. 304 с.
17. *Маховенко Е. Б.* Теоретико-числовые методы в криптографии. М.: Гелиос, 2006. 320 с.
18. *Ниссенбаум О. В., Поляков Н. В.* Криптографические протоколы: лабораторный практикум: учебно-методическое пособие для студентов специальностей «Компьютерная безопасность» и «Информационная безопасность автоматизированных систем». Тюмень: ТюмГУ, 2012. 40 с.

19. *Деза Е. И., Котова, Л. В.* Введение в криптографию: Теоретико-числовые основы защиты информации. (Основы защиты информации № 14). М.: ЛЕНАНД, 2018. 376 с.
20. Федеральный государственный образовательный стандарт среднего общего образования (10–11 кл.). URL: https://fgos.ru/LMS/wm/wm_fgos.php?id=sred (дата обращения: 28.08.2019).
21. *Деза Е. И.* Особенности реализации концепции создания индивидуальных траекторий фундаментальной подготовки учителя математики в условиях вариативного образования // Наука и школа. 2012. № 2. С. 28–34.
22. *Деза Е. И., Котова Л. В., Модель Д. Л.* Современные средства математической подготовки студентов педагогических вузов // Проблемы современного образования. 2018. № 2. С. 147–155.
23. *Деза Е. И., Модель Д. Л.* Особенности построения учебных пособий в условиях интегративно-модульного подхода к обучению дискретной математике // Вестник Московского гор. пед. ун-та. Сер.: Педагогика и психология. 2015. № 4 (34). С. 84–89.
24. *Деза Е. И., Котова Л. В.* Учебные пособия как средство профессионально-ориентированной подготовки студентов // Актуальные проблемы преподавания математики в школе и педвузе: межвуз. сб. науч. ст. М.: МПГУ, 2015. Вып. 25. С. 234–238.

REFERENCES

1. Vasilenko O. N. *Teoretiko-chislovye algoritmy v kriptografii.* Moscow, 2003. 328 p.
2. Nesterenko A. Yu. *Teoretiko-chislovye algoritmy v kriptografii.* Moscow, 2012. 224 p.
3. Koblits N. *Kurs teorii chisel i kriptografii.* Moscow: Nauchnoe izd-vo TVP, 2001. 260 p.
4. Ryabko B. Ya., Fionov A. N. *Osnovy sovremennoy kriptografii i steganografii.* Moscow: Goryachaya liniya-Telekom, 2011. 232 p.
5. Schneier B. *Prikladnaya kriptografiya.* Moscow: Triumf, 2002. 816 p. (in Russian)
6. Ball W., Coxeter G. *Matematicheskie esse i razvlecheniya.* Moscow: Mir, 1986. 472 p. (in Russian)
7. Yashchenko V. V. (ed.) *Vvedenie v kriptigrafiyu.* Moscow: MTsNMO, 2012. 348 p.
8. Gardner M. *Ot mozaik Penrouza k nadezhnym shifram.* Moscow: Mir, 1993. 416 p. (in Russian)
9. Gomez J. *Mir matematiki. Matematiki, shpiony i khakery. Kodirovanie i kriptografiya.* Moscow: De Agostini, 2014. 144 p. (in Russian)
10. Dorichenko S. Ya., Yashchenko V. V. *25 etyudov o shifrakh.* Moscow: TEIS, 1994. 69 p.
11. Kotova L. V. *Rabochaya programma distsipliny "Metody i sredstva zashchity informatsii". Napravlenie podgotovki: 050100.62 Pedagogicheskoe obrazovanie. Profil podgotovki: Informatika.* Moscow: MPGU, 2012. 24 p.
12. Grinko D. I. Programma mezhdistsiplinarnogo kursa DK.02.01. Kriptograficheskaya zashchita informatsii. *Available at:* http://www.informio.ru/fond/2677/Programma-mezhdisciplinarnogo-kursa-MDK0201-Kriptograficheskaja-zashita-informacii (accessed: 30.07.2019).
13. Kalinin I. A., Samylkina N. N. *UMK „Informatika", 10–11 klassy. Uglublennyy uroven.* Moscow: Binom, 2014. 344 p.
14. Bosova L. L., Bosova A. Yu. *Informatika: uchebnik dlya 5 klassa.* Moscow: Binom, 2015. 184 p.
15. Ugrinovich N. D. *Informatika. Uchebnik dlya 10–11 kl.* Moscow: Laboratoriya Bazovykh Znaniy, 2011. 512 p.
16. Makarova N. V. *Informatika. 10–11 klass.* St. Petersburg: PiterKom, 1999. 304 p.
17. Makhovenko E. B. *Teoretiko-chislovye metody v kriptografii.* Moscow: Gelios, 2006. 320 p.
18. Nissenbaum O. V., Polyakov N. V. *Kriptograficheskie protokoly: laboratornyy praktikum: uchebno-metodicheskoe posobie dlya studentov spetsialnostey „Kompyuternaya*

bezopasnost" i „Informatsionnaya bezopasnost avtomatizirovannykh sistem". Tyumen: TyumGU, 2012. 40 p.
19. Deza E. I., Kotova, L. V. *Vvedenie v kriptografiyu: Teoretiko-chislovye osnovy zashchity informatsii. (Osnovy zashchity informatsii No. 14)*. Moscow: LENAND, 2018. 376 p.
20. Federalnyy gosudarstvennyy obrazovatelnyy standart srednego obshchego obrazovaniya (10–11 kl.). *Available at:* https://fgos.ru/LMS/wm/wm_fgos.php?id=sred (accessed: 28.08.2019).
21. Deza E. I. Osobennosti realizatsii kontseptsii sozdaniya individualnykh traektoriy fundamentalnoy podgotovki uchitelya matematiki v usloviyakh variativnogo obrazovaniya. *Nauka i shkola.* 2012, No. 2, pp. 28–34.
22. Deza E. I., Kotova L. V., Model D. L. Sovremennye sredstva matematicheskoy podgotovki studentov pedagogicheskikh vuzov. *Problemy sovremennogo obrazovaniya.* 2018, No. 2, pp. 147–155.
23. Deza E. I., Model D. L. Osobennosti postroeniya uchebnykh posobiy v usloviyakh integrativno-modulnogo podkhoda k obucheniyu diskretnoy matematike. *Vestnik Moskovskogo gor. ped. un-ta. Ser.: Pedagogika i psikhologiya.* 2015, No. 4 (34), pp. 84–89.
24. Deza E. I., Kotova L. V. Uchebnye posobiya kak sredstvo professionalno-orientirovannoy podgotovki studentov. In: *Aktualnye problemy prepodavaniya matematiki v shkole i pedvuze. Interuniv. coll. of scient. art.* Moscow: MPGU, 2015. Iss. 25. Pp. 234–238.

Деза Елена Ивановна, кандидат физико-математических наук, доктор педагогических наук, доцент, профессор кафедры теоретической информатики и дискретной математики Института математики и информатики Московского педагогического государственного университета

e-mail: Elena.Deza@gmail.com

Deza Elena I., PhD in Physics and Mathematics, ScD in Education, Associate professor, Professor, Theoretical Informatics and Discrete Mathematics Department, Institute of Mathematics and Informatics, Moscow Pedagogical State University

e-mail: Elena.Deza@gmail.com

Котова Лидия Владимировна, кандидат педагогических наук, доцент кафедры теории чисел Института математики и информатики Московского педагогического государственного университета

e-mail: kolv@inbox.ru

Kotova Lidia V., PhD in Education, Associate Professor, Number Theory Department, Institute of Mathematics and Informatics, Moscow Pedagogical State University

e-mail: kolv@inbox.ru

Лебедева Елена Сергеевна, старший преподаватель кафедры общеобразовательных дисциплин Российского государственного университета правосудия

e-mail: v_les@rambler.ru

Lebedeva Elena S., Senior Lecturer, General Educational Subjects Department, Russian State University of Justice

e-mail: v_les@rambler.ru

Статья поступила в редакцию 29.08.2019
The article was received on 29.08.2019