13. Chegodayev A. I. Matematicheskiye metody analiza ekspertnykh otsenok [Mathematical methods for analyzing expert assessments]. *Vestnik Samarskogo gosudarstvennogo ekonomicheskogo universiteta* [Bulletin of Samara State University of Economics], 2010, no. 2, pp. 130–135.

14. Yarushkina, N.G. *Nechetkie gibridnye sistemy. Teoriya i praktika* [Fuzzy hybrid systems. Theory and practice]. Moscow, Fizmatlit Publ., 2007. 208 p.

15. Biswas R. An application of fuzzy sets in students' evaluation. *Fuzzy Sets and Systems*, 1995, no. 74 (2), pp. 187–194.

16. Feden P. D., Vogel R. M. *Methods of teaching. Applying cognitive science to promote student learning*. New York, Mc Graw-Hill, 2003, pp. 257–302.

17. Piegat Andrzej. *Fuzzy Modeling and Control: with 96 tables*. Heidelberg; New York, Physica-Verl., 2001.

18. Zadeh L. A. Fuzzy sets. *Information and Control*, 1965, no. 8, pp. 338–353.

УДК 004.588

ОБЕСПЕЧЕНИЕ КОМПЕТЕНТНОСТИ РОССИЙСКИХ ШКОЛЬНИКОВ В ВОПРОСАХ КРИПТОГРАФИИ: АНАЛИЗ ЦЕЛЕЙ, ВОЗМОЖНЫХ ПОДХОДОВ И ТЕХНОЛОГИЙ, СРЕДСТВ ИХ ПРОГРАММНОЙ ПОДДЕРЖКИ

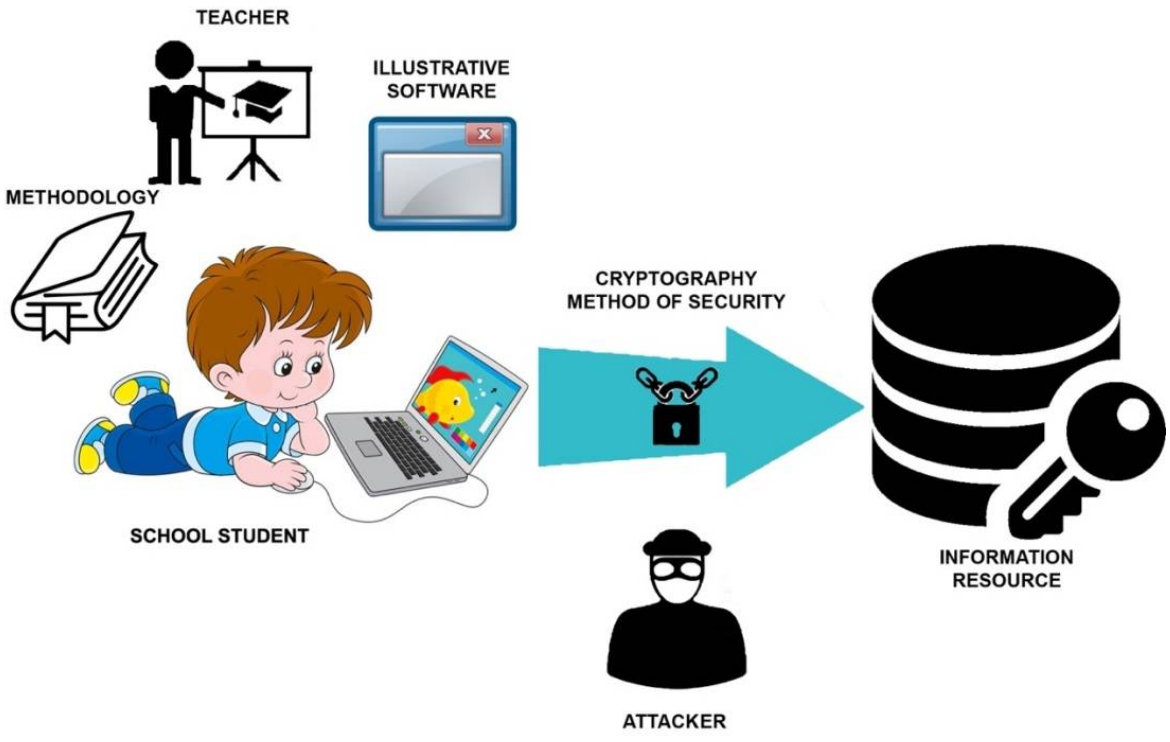
Статья поступила в редакцию 15.05.2019, в окончательном варианте – 04.06.2019.

Кузнецова Валентина Юрьевна, Астраханский государственный университет, 414056, Российская Федерация, г. Астрахань, ул. Татищева, 20а,
магистрант, e-mail: arhelia@bk.ru

Показана роль обучения криптографическим методам защиты информации школьников как активных пользователей глобальной сети интернет. С позиций государства, общества, родителей и самих школьников рассмотрены цели повышения уровня компетентности несовершеннолетних в вопросах информационной безопасности. Проанализировано существующее положение в сфере образовательной политики в вопросе обучения криптографии и выявлены недостатки. Предложены методические рекомендации по обучению криптопримитивам (шифры перестановки, подстановки, аналитические преобразования и гаммирование) с использованием учебно-демонстрационного программного продукта. Показаны функциональные возможности и результативность описываемого программного продукта в целях обеспечения компетентности школьников в вопросах криптографии.

Ключевые слова: криптография, информационная безопасность, общее образование, обучение криптографии, системное мышление, программный продукт

Графическая аннотация (Graphical annotation)



THE ENSURING COMPETENCE OF RUSSIAN STUDENTS IN CRYPTOGRAPHY ISSUES: ANALYSIS OF PURPOSES, POSSIBLE APPROACHES, MEANS OF THEIR SOFTWARE SUPPORT

The article was received by editorial board on 15.05.2019, in the final version – 04.06.2019.

Kuznetsova Valentina Yu., Astrakhan State University, 20a Tatishchev St., Astrakhan, 414056, Russian Federation,
undergraduate student, e-mail: arhelia@bk.ru

In this article are proved the role of teaching cryptographic methods of protecting information of schoolchildren as active users of the global Internet. From the standpoint of the state, society, parents and students, the goals of raising the level of competence of minors in matters of information security were considered. Analyzed the existing situation in the field of educational policy in the issue of cryptography training and identified shortcomings. Methodical recommendations for teaching cryptoprimitives are proposed (permutation ciphers, substitutions, analytical transformations and gamming) using training and demonstration software. The functional capabilities and effectiveness of the described software product are shown in order to ensure the competence of students in cryptography issues.

Keywords: cryptography, information security, general education, cryptography training, system thinking, educational and demonstration software

Введение. В последние годы во всем мире, и в том числе в России, наука «криптография» стала интенсивно развиваться как повсеместно используемая во всех сферах жизни общества. Она легла в основу многих областей комплексной защиты информации государственных, экономических и военных информационных ресурсов, а также в повседневных бытовых вопросах. Криптографические методы защиты информации используются при личной переписке посредством электронной почты, при использовании систем онлайн-банкинга, электронного документооборота и т.п. И перечисленными системами уже активно пользуются школьники, которые чаще всего и становятся жертвами угроз, связанных с детской невнимательностью, наивностью и некомпетентностью в вопросах информационной безопасности.

Информационная безопасность подрастающего поколения – приоритетная задача государства, и если всего лишь пару лет назад правила безопасного использования интернета обсуждались только со студентами и старшеклассниками, то уже сейчас с интенсивной информатизацией общества (по данным Росстата, общее количество домашних хозяйств с доступом в интернет за последние 3 года выросло в среднем на 4 %, из них с помощью мобильного устройства на 15 %) активными пользователями глобальной сети становятся дети в возрасте 9–12 лет и их взросление происходит неразрывно от технологий. Но при всем этом уровень компетентности в сфере информационной безопасности (ИБ) у юных пользователей недостаточный для того, чтобы безопасно использовать привычные и наиболее популярные информационные ресурсы. Это подтверждает статистика: с 2014 г. растет количество преступлений, совершенное против несовершеннолетних, 44 % несовершеннолетних пользователей интернета хотя бы раз подвергались в сети сексуальным домогательствам, жертвами интернет-мошенников, в том числе при совершении онлайн-платежей, становились 54 % опрошенных детей в возрасте до 18 лет [16].

На основании вышеизложенного целью данной работы стал анализ текущего уровня компетентности в вопросах информационной безопасности и криптографии для формирования рекомендаций по методам и средствам его повышения.

Позиция лиц, заинтересованных в компетентности школьников. Информационная безопасность всеобъемлюще охватывает все области общественной жизни, поэтому компетенции в сфере защиты информации требуются не только для будущих IT-инженеров, но и для специалистов любых сфер деятельности, так как методами и средствами защиты информации должны сейчас уметь пользоваться любые пользователи персональных компьютеров. Именно поэтому затрагивать данный вопрос необходимо начиная с начальной школы. Это подтверждают и психологи, которые также утверждают, что именно в этом возрасте начинает формироваться системное мышление, на которое оказывает влияние изучение основ информационной безопасности и криптографии как ее ключевого элемента. Данный эффект, по мнению исследователей, основан на том, что занятия криптографией развивают у ребенка логику, умение связывать между собой в целостную систему определенные признаки, видеть и подмечать отдельные существенные элементы.

С позиции государства, родителей и общества повышение уровня компетентности школьников в вопросах ИБ поможет сократить количество преступлений, связанных с интернет-мошенничеством, потому что именно дети в силу своей доверчивости и невнимательности чаще всего становятся жертвами фишинговых сайтов, мошеннических платежных систем и прочих противоправных действий. Кроме того, это может предотвратить похищения и ограбления, так как большинство этих преступлений совершаются в результате необдуманных действий со стороны детей – публикация фотографий новых мобильных телефонов, домашних адресов и прочей личной информации, которой пользуются злоумышленники.

Вопросы криптографии в системе школьного образования России. Несмотря на заинтересованность государства в обеспечении должного уровня компетентности школьников в вопросах криптографии как основного метода обеспечения конфиденциальности, аутентичности и неотказуемости, в отечественной образовательной практике некоторые вопросы, связанные с криптографией, рассматриваются лишь частично в рамках школьного курса информатики при изучении тем, связанных с кодированием. Специальный курс криптографии как отдельный предмет или хотя бы более полный раздел в рамках курса информатики в федеральном образовательном стандарте и примерной учебной программе отсутствует.

Вопросы, связанные с криптографией, согласно поурочному календарно-тематического планированию, обычно рассматриваются в учебниках следующих классов.

В программах учебников информатики 2-го, 3-го, 5-го классов (рабочая программа по учебникам Н.В. Матвеевой, рассчитанная на 35 часов) [7] школьникам преподают шифрование на примере шифра Цезаря вместе с двоичным кодированием, при этом учащимся не дается пояснение о разнице этих понятий. В результате этого в сознании учащихся шифрование становится тождественным кодированию, что является абсолютно ошибочным. Например, азбука Морзе, являясь всемирно известным способом знакового кодирования, обеспечивает удобство передачи информации по линиям связи, в то время как криптоалгоритмы служат для обеспечения конфиденциальности хранимой и передаваемой информации.

В учебниках 10 класса И.Г. Семакина (углубленное изучение информатики) [6] в разделе «Информационные процессы в системах» среди мер защиты информации обзорно рассказывается о криптографии как науке, кратко описывается история развития криптографии, упоминается ассиметричное шифрование для введения термина «цифровая подпись». Наравне с этим дается определение закрытого ключа в симметричных криптосистемах (отождествляя его с ключом симметричного шифрования), что является неточностью и вводит в заблуждение учащихся. Понятие закрытого ключа правильно использовать только при обсуждении ассиметричных криптосистем. Для закрепления изученного материала в списке практических работ имеется тема «Шифрование данных», где учащимся необходимо решить задачи, связанные с шифрами Цезаря, Виженера, безымянными шифрами перестановки, которые не рассматривались в теоретическом материале. При этом авторы-составители ошибочно используют термины «декодирование» в значении «расшифрование».

В учебнике информатики для 11-го класса вопрос криптографии включен в урок по теме «Организация защиты информации. Антивирусная защита информации» (программа по учебникам И.Г. Семакина углубленного уровня) [11]. По аналогии с учебником 10-го класса, в нем допускается ошибка отождествления шифрования и кодирования: автор дает определение: «шифрование – это кодирование специального вида». Также вводится определение криптоанализа и ключей шифрования. В параграфе рассматривается более подробно шифр Цезаря и описывается механизм шифрования методом Виженера. Для закрепления материала учащимся предлагается решить 6 задач на оба метода шифрования.

Криптографию в школах обычно выводят за рамки образовательной программы и оставляют в качестве элементов внеурочной деятельности – факультативов и кружков. Издательство «Бином» в 2014 г. предлагало учителям организовывать внеурочную деятельность на основе предложенных ими учебно-методических комплектов. Один из них – учебное пособие Э.В. Тановой «Введение в криптографию: как защитить свое письмо от любопытных» [13]. Автор разработала элективный курс с подробной рабочей программой, методическими материалами и книгой для ученика и учителя. При этом изучение криптографии в рамках школьного образования различного уровня более подробно рассматривается в ее диссертационной работе [14].

Таким образом, приходится констатировать, что полноценные методические и дидактические материалы для проведения занятий по криптографии со школьниками отсутствуют. Каждый педагог на свое усмотрение подбирает материал по тому или иному шифру, ориентируясь исключительно на собственные предпочтения или опыт. Электронные ресурсы для программной поддержки обучения криптографии также не разрабатывались.

Анализ уровня компетентности школьников в вопросах криптографии. Для анализа уровня компетентности школьников в вопросах информационной безопасности была сформирована случайным образом экспериментальная группа учащихся 7–9 классов технологического профиля средней школы города Астрахани в количестве 60 человек. Сбор данных осуществлялся с помощью тестирования. Тест проходил в письменной форме и состоял из 40 вопросов, 10 вопросов по каждой из тем – программно-аппаратные средства защиты информации (ЗИ), инженерно-технические, организационно-правовые, криптографические. На решение тестов школьникам отводилось 30 минут. Каждый блок заданий оценивался по стобалльной шкале [8].

По результатам первичного среза выяснилось, что некоторые вопросы информационной безопасности для школьников были знакомы, такие как антивирусная защита, принципы парольной защиты, так как эти вопросы частично затрагиваются в рамках школьного курса информатики. Однако криптографические методы учащимися были практически не изучены (табл. 1).

Таблица 1 – Результаты первичного среза знаний по основным разделам курса информационной безопасности

Методы ЗИ	**7 класс**	**8 класс**	**9 класс**
Программно-аппаратные	32,7	43,6	52,3
Инженерно-технические	45,8	54,2	59,4
Организационно-правовые	33,9	34,6	36,2
Криптографические	13,2	14,7	15,2

Из таблицы можно заметить, что средний балл знаний криптографических мер защиты информации в среднем в 2–3 ниже, чем по остальным мерам обеспечения информационной безопасности.

В связи с вышесказанным был разработан и проведен факультативный курс по основам криптографической защиты информации для учащихся 7–9 классов средней школы. Рабочая программа данного факультативного курса включала 36 часов аудиторных занятий, из них 12 – лекции, 18 часов – практических уроков, 6 часов выделено для проведения самостоятельных и контрольных работ.

Занятия проводились по одному разу в неделю в группах количеством двадцать человек, отдельно для седьмых, восьмых и девятых классов. Всего в занятиях факультативного курса приняли участие 60 человек.

С учащимися были рассмотрены четыре вида криптографических преобразований – перестановка, подстановка (замена), гаммирование и аналитические преобразования. И если шифры простой перестановки и шифр Цезаря не вызывали особых трудностей у учащихся, то более сложные криптопримитивы (шифр Виженера, криптосистема Хилла и т.п.) требовали более тщательной проработки и грамотного подобранных демонстрационных материалов.

При проведении факультативного курса стало очевидным, что для освоения элементарных криптографических докопьютерных преобразований не хватает наглядно-демонстрационного материала, который бы поспособствовал лучшему усвоению механизмов шифрования.

Средство программной поддержки изучения факультативного курса. После анализа отечественного и зарубежного опыта [5] внедрения криптографии в программу средней школы стало очевидно, что из электронных образовательных ресурсов по криптографии имеются только электронные презентации и тесты, реализованные с помощью электронных книг на базе программного пакета Microsoft Office. Поэтому было принято решение разработать собственный демонстрационно-обучающий программный продукт [4].

Программный продукт написан на языке объектно-ориентированного программирования C# с помощью среды Visual Studio 2012 при использовании офисного пакета Microsoft Office 2019 для представления теоретических сведений. ПО предназначено для установки на персональных компьютерах с операционной системой Windows 7 и выше.

Он отличается интуитивно понятным интерфейсом и яркими демонстрационными элементами (рис. 1). Это способствует быстрому освоению алгоритмов шифрования.

Данный продукт является учебно-демонстрационным, иллюстративным средством самоконтроля и не предназначен для дистанционного обучения. Его рекомендуется использовать как вспомогательное средство для изучения криптографических преобразований в рамках факультативного курса.

Программный продукт предусматривает три режима работы – изучение теоретической информации (презентации в формате Power Point), режим «Демонстрация» (побуквенная демонстрация работы шифра и мгновенное шифрование) и режим «Проверка», когда учащийся самостоятельно может проверить свой шифротекст на предмет правильности осуществленных преобразований.

Освоение криптографических преобразований с помощью ПО предусматривает ознакомление с теоретической базой и математическими основами элементарных криптопреобразований (перестановки, подстановки (замены), аналитического преобразования и гаммирования) на примере работы с демонстрационными вариантами реализации конкретных криптосистем (рис. 2).

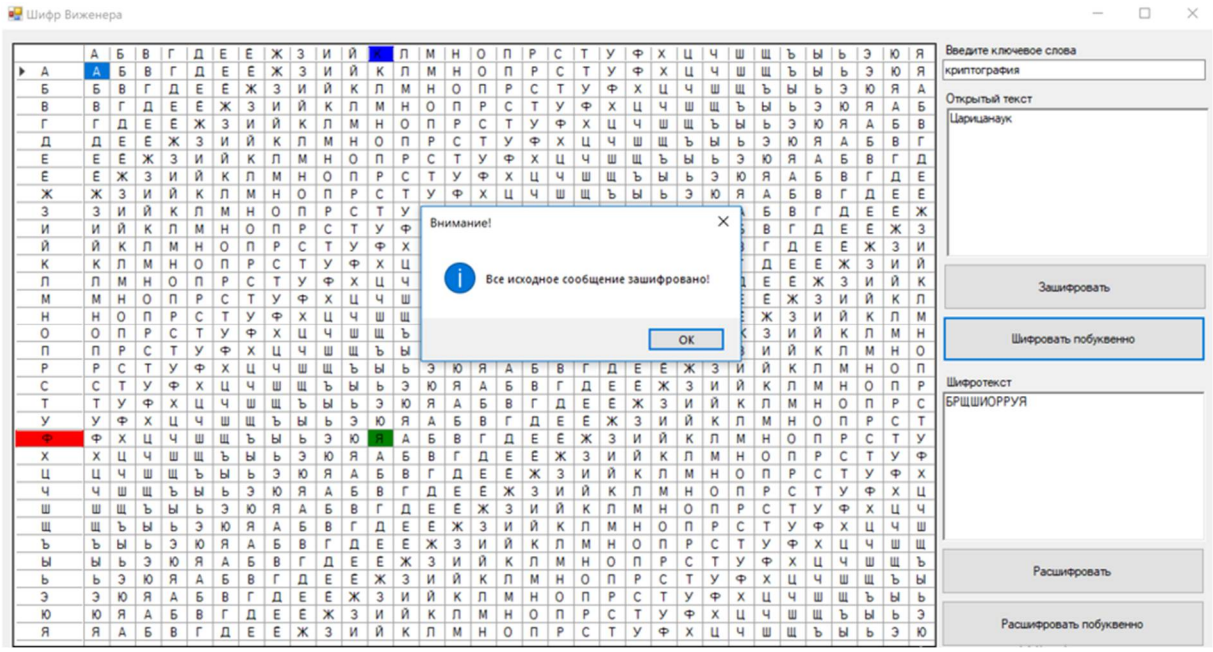


Рисунок 1 – Интерфейс демонстрации работы шифра Виженера в режиме побуквенного шифрования

Рисунок 2 – Интерфейс программного продукта, демонстрирующий четыре вида криптографических преобразований

Шифры перестановки демонстрируются на примере реализации криптоалгоритмов «Двойная перестановка» и «Магический квадрат» [6].

Шифры подстановки проиллюстрированы алгоритмами «Двойной квадрат Уитстона» и шифром Виженера.

Гаммирование демонстрируется на примере реализации шифра Вернама.

В качестве примера шифра, использующего аналитическое преобразование, приведена реализация криптосистемы Хилла.

Каждый рассмотренный шифр в режиме теоретических сведений сопровождается презентацией (всего 6 презентаций по 13–17 слайдов).

Данная последовательность (рис. 3) изучения методов шифрования связана с принципом «от простого к сложному»: шифры перестановки интуитивно понятны школьникам и не вызывают затруднений, в то время как шифры гаммирования и аналитических преобразований требуют знания математического аппарата и к тому же в какой-то степени базируются на шифрах перестановки и простой замены [2].

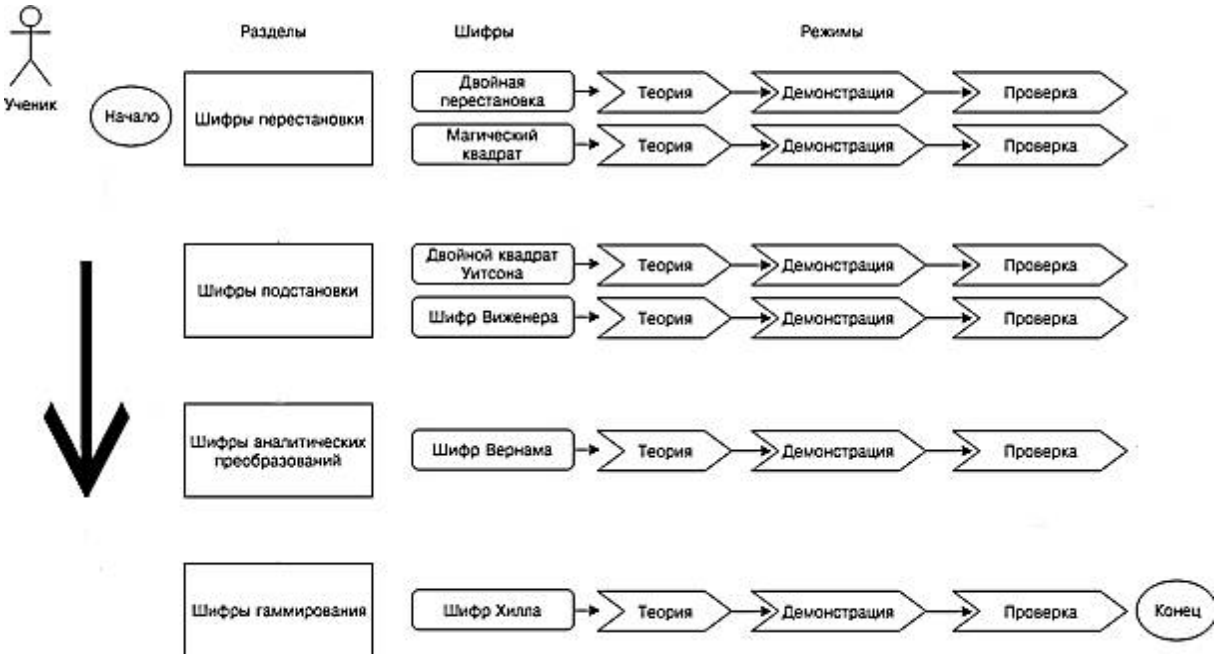


Рисунок 3 – Последовательность изучения методов криптографии с помощью разработанного ПО

Апробация эффективности использования программного продукта проводилась с помощью экспериментальной и контрольной групп в 9 классе. Группу из 20 человек случайным образом разделили пополам: экспериментальная группа изучала криптографические преобразования с использованием учебно-демонстрационной программы, контрольная – без нее – все остальные дидактические материалы (презентационные материалы, тесты, самостоятельные и контрольные работы) у обеих групп были одинаковые [3, 12].

После завершения обучения учащимся обеих групп была предложена контрольная работа из 6 задач по различным видам криптопреобразований. В итоге были получены следующие результаты (табл. 2).

Таблица 2 – Результаты для экспериментальной и контрольной групп обучавшихся

Оценка в баллах	Количество учащихся	
	Экспериментальная группа	Контрольная группа
90–100	6	3
80–89	5	5
70–79	2	4
0–69	0	1

Таким образом, наглядно продемонстрировано, что обучение криптографии с помощью учебно-демонстрационного программного продукта дало лучшие результаты.

Заключение. Чтобы обучение проходило в режиме онлайн без необходимости установки программного продукта на рабочую станцию, планируется модернизировать программный продукт, реализовав в нем режимы тестирования и проверки знаний для контроля учителем. Планируется также создать на базе описанного программного продукта онлайн-ресурс.

Библиографический список

1. Душкин Р. Математика и криптография. Тайны шифров и логическое мышление / Р. Душкин ; под ред. А. Амелькиной. – Москва : АСТ, 2017. – 288 с.

2. Кузнецова В. Ю. Методические аспекты обучения симметричным шифрам в рамках факультативного курса криптографии для школьников / В. Ю. Кузнецова // Симметрии: теоретический и методический аспекты : сборник научных трудов VII Международной научно-практической конференции : в 2 т. – Астрахань : ООО ПКФ «Триада», 2018. – Т. 1. – С. 203–207.

3. Кузнецова В. Ю. Использование онлайн-кроссвордов для реализации смешанного обучения криптографии / В. Ю. Кузнецова // Модернизация системы непрерывного образования : материалы IX Международной научно-практической конференции. – Махачкала, 2017. – С. 267–270.

4. Кузнецова В. Ю. Использование учебно-демонстрационной программы с целью обучения школьников криптографии / В. Ю. Кузнецова // Образование в цифровую эпоху: проблемы и перспективы : материалы Международной научно-практической конференции. – Астрахань : Астраханский государственный университет, 2019. – С. 16–20.

5. Кузнецова В. Ю. Российский и зарубежный опыт внедрения дисциплины «криптография» в программу средней школы / В. Ю. Кузнецова, А. В. Станишевская // Проблемы информационной безопасности : материалы. – Ростов н/Д. : Азов-Принт, 2018. – С. 108–112.

6. Лэнс Бриант. Шифр Цезаря: введение в криптографию / Лэнс Бриант. – Режим доступа:http://www.purdue.edu/discoverypark/gk12/downloads/Cryptography.pdf, свободный. – Заглавие с экрана. – Яз. англ. (дата обращения 21.11.2018).

7. Матвеева Н. В. Авторская мастерская / Н. В. Матвеева. – Режим доступа: http://lbz.ru/metodist/authors/informatika/4/, свободный. – Заглавие с экрана. – Яз. рус. (дата обращения 27.02.2019).

8. Отрывашкина Т. М. Подготовка учащихся средней школы к решению криптографических задач / Т. М. Отрывашкина. – Режим доступа: http://elib.osu.ru/bitstream/123456789/1377/1/2772-2775.pdf, свободный. – Заглавие с экрана. – Яз. рус. (дата обращения 21.11.2017).

9. Приказ Минобрнауки России от 17 декабря 2010 г. № 1897 «Об утверждении федерального государственного образовательного стандарта основного общего образования». – Режим доступа: http://www.edu.ru/db-mon/mo/Data/d_10/m1897.html, свободный. – Заглавие с экрана. – Яз. рус. (дата обращения 28.03.2019).

10. Приказ Минобрнауки России от 29 декабря 2014 г. № 1644 «О внесении изменений в федеральный государственный образовательный стандарт основного общего образования, утверждённый приказом Министерства образования и науки Российской Федерации от 17 декабря 2010 г. № 1897». – Режим доступа: http://минобрнауки.рф/документы/543, свободный. – Заглавие с экрана. – Яз. рус. (дата обращения 28.03.2019).

11. Семакин И. Г. Авторская мастерская / И. Г. Семакин. – Режим доступа: http://lbz.ru/metodist/authors/informatika/2/, свободный. – Заглавие с экрана. – Яз. рус. (дата обращения 27.02.2019).

12. Смирнова М. О. Проектная деятельность при изучении криптографии в средней школе / М. О. Смирнова, В. Ю. Кузнецова // Проектная деятельность: новый взгляд на образование : сборник трудов Всероссийской научно-практической конференции. 24–25 апреля 2018 г. – Астрахань : Астраханский государственный университет, Издательский дом «Астраханский университет», 2018. – С. 212–216.

13. Танова Э. В. Формирование компетентности в области защиты информации у школьников в процессе обучения информатике : дис. … канд. пед. наук / Э. В. Танова. – Челябинск : Челяб. гос. пед. университет, 2005. – 173 с.

14. Танова Э. В. Введение в криптографию: как защитить свое письмо от любопытных : учебное пособие / Э. В. Танова. – Москва : Бином. Лаборатория знаний, 2007. – 198 с.

15. Федеральный государственный образовательный стандарт основного общего образования (5–9 кл.) (ФГОС ООО) – Режим доступа: http://www.edu.ru/db-mon/mo/Data/d_10/prm1897-1.pdf, свободный. – Заглавие с экрана. – Яз. рус. (дата обращения 05.05.2019).

16. Майкулов Ж. Ж. Преступления против детей с использованием Интернета / Ж. Ж. Майкулов // Концепт : научно-методический электронный журнал. – 2017. – Т. 39. – С. 2636–2640. – Режим доступа: http://e-koncept.ru/2017/970854.htm, свободный. – Заглавие с экрана. – Яз. рус.

References

1. Dushkin R. *Matematika i kriptografiya. Tayny shifrov i logicheskoe myshlenie* [Math and cryptography. Cipher secrets and logical thinking]. Moscow, AST Publ., 2017. 288 p.

2. Kuznetsova V. Yu. Metodicheskie aspekty obucheniya simmetrichnym shifram v ramkah fakultativnogo kursa kriptografii dlya shkolnikov [Methodical aspects of training of the symmetric ciphers within an optional course for students of cryptography]. *Simmetrii: teoreticheskiy i metodicheskiy aspekty : sbornik nauchnykh trudov VII Mezhdunarodnoy nauchno-prakticheskoy konferentsii* [The symmetry: theoretical and methodical aspects : Proceedings of the VII International Scientific and Practical Conference], in 2 vol. Astrakhan, "Triada" PKF Ltd. Publ., 2018, vol. 1, pp. 203–207.

3. Kuznetsova V. Yu. Ispolzovanie onlayn-krossvordov dlya realizatsii smeshannogo obucheniya kriptografii [The using of online crosswords for the implementation of blended learning of cryptography]. *Modernizaciya sistemy nepreryvnogo obrazovaniya : materialy IX Mezhdunarodnoy nauchno-prakticheskoy konferentsii* [Modernization of the system of continuous education : Proceedings of the IX International Scientific and Practical Conference]. Mahachkala, 2017, pp. 267–270.

4. Kuznetsova V. Yu. Ispolzovanie uchebno-demonstracionnoy programmy s tselyu obucheniya shkolnikov kriptografii [The using of the illustrative software for teaching cryptography to schoolchildren]. *Obrazovanie v tsifrovuyu epokhu: problemy i perspektivy : materialy Mezhdunarodnoy nauchno-prakticheskoy konferentsii* [Education in the digital age: problems and prospects : Materials of the International Scientific and Practical Conference]. Astrakhan, Astrakhan State University Publ., 2019, pp. 16–20.

5. Kuznetsova V. Yu., Stanishevskaya A. V. Rossiyskiy i zarubezhnyy opyt vnedreniya discipliny «kriptografiya» v programmu sredney shkoly [Russian and foreign experience of introducing the discipline "cryptography" to the secondary school program]. *Problemy informatsionnoy bezopasnosti: materialy* [Problems of information security : materials]. Rostov-on-Don, Azov-Print Publ., 2018, pp. 108–112.

6. Lens Briant. *Shifr Tsezarya: vvedenie v kriptografiyu* [Caesar cipher: an introduction to cryptography.] Available at: http://www.purdue.edu/discoverypark/gk12/downloads/Cryptography.pdf (accessed 17.03.2019).

7. Matveeva N. V. *Avtorskaya masterskaya* [The Author's online-workshop]. Available at: http://lbz.ru/metodist/authors/informatika/4/ (accessed 27.02.2019).

8. Otryvashkina T. M. *Podgotovka uchashchikhsya sredney shkoly k resheniyu kriptograficheskikh zadach* [Preparing high school students for solving cryptographic tasks]. Available at: http://elib.osu.ru/bitstream/123456789/1377/1/2772-2775.pdf (accessed 21.11.2017).

9. *Prikaz Minobrnauki Rossii ot 17 dekabrya 2010 g. № 1897 «Ob utverzhdenii federalnogo gosudarstvennogo obrazovatelnogo standarta osnovnogo obshchego obrazovaniya»* [Order of the Ministry of Education and Science of Russia

dated December 17, 2010 no. 1897 “On approval of the federal state educational standard of basic general education”]. Available at: http://www.edu.ru/db-mon/mo/Data/d_10/m1897.html (accessed 28.03.2019).

10. *Prikaz Minobrnauki Rossii ot 29 dekabrya 2014 g. № 1644 «O vnesenii izmeneniy v federalnyy gosudarstvennyy obrazovatelnyy standart osnovnogo obshchego obrazovaniya, utverzhdyonnyy prikazom Ministerstva obrazovaniya i nauki Rossiyskoy Federatsii ot 17 dekabrya 2010 g. № 1897»* [Order of the Ministry of Education and Science of Russia of December 29, 2014 No. 1644 “On Amendments to the Federal State Educational Standard of Basic General Education, approved by Order of the Ministry of Education and Science of the Russian Federation of December 17, 2010 no. 1897]. Available at: http://minobrnauki.rf/dokumenty/543 (accessed 28.03.2019).

11. Semakin I. G. *Avtorskaya masterskaya* [The Author's online-workshop]. Available at: http://lbz.ru/metodist/authors/informatika/2/ (accessed 27.02.2019).

12. Smirnova M. O., Kuznetsova V. Yu. Proektnaya deyatelnost pri izuchenii kriptografii v sredney shkole [The project activity at the studing of cryptography in the second school]. *Proektnaya deyatelnost: novyy vzglyad na obrazovanie : sbornik trudov Vserossiyskoy nauchno-prakticheskoy konferentsii* [Project activity: a new look at education: a collection of works of the All-Russian scientific-practical conference]. Astrakhan, Astrakhan State University, Publishing House “Astrakhan University”], 2018, pp. 212–216.

13. Tanova E. V. *Formirovanie kompetentnosti v oblasti zashchity informatsii u shkolnikov v processe obucheniya informatike* [Formation of competence in the field of information security among schoolchildren in the process of teaching computer science]. Chelyabinsk, Chelyabinsk State Pedagogical University, 2005.

14. Tanova E. V. *Vvedenie v kriptografiyu: kak zashchitit svoe pismo ot lyubopytnykh: uchebnoe posobie* [Introduction to cryptography: how to protect your letter from the curious: study guide]. Moscow, Binom. Laboratoriya znaniy Publ., 2007. 173 p.

15. *Federalnyy gosudarstvennyy obrazovatelnyy standart osnovnogo obshchego obrazovaniya (5–9 kl.)* [Federal State Educational Standard of Basic General Education (5–9 cl.)]. Available at: http://www.edu.ru/db-mon/mo/Data/d_10/prm1897-1.pdf (accessed 05.05.2019).

16. Maykulov Zh. Zh. Prestupleniya protiv detey s ispolzovaniem Interneta [The crimes against children using the Internet]. *Kontsept : nauchno-metodicheskiy elektronnyy zhurnal* [Concept : scientific-methodical electronic journal], 2017, vol. 39, pp. 2636–2640. Available at: http://e-koncept.ru/2017/970854.htm.

УДК 004.422

IDENTIFICATION OF PERSONALITY BASED ON ELECTRONIC DOCUMENTS WITH INCREASED SECURITY LEVEL

The article was received by editorial board on 22.03.2019, in the final version – 31.05.2019.

Azhmukhamedov Iskandar M., Astrakhan State University, 20a Tatishchev St., Astrakhan, 414056, Russian Federation,
Doct. Sci. (Engineering), Professor, e-mail: iskander_agm@mail.ru
Poletayev Nikita S., Astrakhan State University, 20a Tatishchev St., Astrakhan, 414056, Russian Federation,
student, e-mail: npoletaev97@gmail.com
Stanishevskaya Alina V., Astrakhan State Technical University, 16 Tatishchev St., Astrakhan, 414056, Russian Federation,
undergraduate student, e-mail: a.stanishevskaia@gmail.com

Identity documents play a big role in ensuring personal and public safety. However, the most widely used paper documents today have significant drawbacks. To eliminate them, a technique has been proposed that involves the combined use of steganographic and cryptographic algorithms. This paper describes approaches to the implementation of software that allows in practice to implement this technique. There are three main modules in the software: data encryption module; steganographic data embedding module in the image; a module for recording generated data on a smart card. Using the developed software allows you to get an identity document with a high level of protection from attacks on its integrity and the inability to use third parties, because without knowing the key, part of which is known only to the owner, and the other part is stored in the database of the public authority, it is impossible to decipher the embedded information.

Keywords: electronic identification card, robust steganography algorithm, data flow diagram, cryptography, steganography