УДК 373.1:004.056.5

КОНЦЕПТУАЛЬНАЯ МОДЕЛЬ ОБУЧЕНИЯ ОСНОВАМ КИБЕРБЕЗОПАСНОСТИ В ОСНОВНОЙ ШКОЛЕ

Троицкая О.Н.[1], Ширикова Т.С.[1], Безумова О.Л.[1], Лыткина Е.А.[1]

[1]ФГАОУ ВО «Северный (Арктический) федеральный университет имени М.В. Ломоносова», Архангельск, e-mail: o.troitskaya@narfu.ru

Статья посвящена решению вопроса создания концептуальной модели обучения основам кибербезопасности учащихся основной школы. Проведен сравнительный анализ понятий «информационная безопасность» и «кибербезопасность» в нормативных документах. На основе анализа опыта разработчиков программного обеспечения и учителей выявлены цель и средства обучения основам кибербезопасности. В статье описаны недостатки программы Л.Л. Босовой, по которой работают многие учителя информатики в 5-9 классах, в аспекте обучения основам кибербезопасности. Так, например, несмотря на описания особенностей работы электронной почты, пятиклассникам не сообщают основные правила создания паролей в киберпространстве, которые позволят им сохранять личную информацию, хранящуюся на почте. В статье описана концептуальная модель обучения основам кибербезопасности учащихся основной школы. Она реализует идею непрерывного обучения кибербезопасности, обеспечит метапредметность результатов обучения, раскроет существующие сегодня киберугрозы и правила действий при встрече с ними. Одной из форм реализации модели является неделя кибербезопасности. В рамках недели планируется проведение классных часов в формате научно-популярных лекций, интерактивных игр, конкурса на лучшее сочинение по теме, раскрывающей особенности кибербезопасности, конкурса рисунков, который позволит раскрыть творческий потенциал детей и отразить их представления о киберпространстве, родительских собраний, тема которых «Кибербезопасность», конкурса задач по кибербезопасности.

Ключевые слова: кибербезопасность, школьники, киберугроза, концептуальная модель, неделя кибербезопасности.

A CONCEPTUAL MODEL OF TEACHING THE BASICS OF CYBERSECURITY IN THE SECONDARY SCHOOL

Troitskaya O.N.[1], Bezumova O.L.[1], Shirikova T.S.[1], Lytkina E.A.[1]

[1]Northern (Arctic) Federal University named after M.V. Lomonosov, Arkhangelsk, e-mail: o.troitskaya@narfu.ru

The article is devoted to the solution of the problem of creating a conceptual model of teaching the basics of cybersecurity of schoolchildren. A comparative analysis of the concepts of “information security” and “cybersecurity” in normative documents was carried out in the article. Based on the analysis of the experience of software developers and teachers it was identified the purpose and means of teaching the basics of cybersecurity. The article describes the shortcomings of the L. L. Bosova's program, which many teachers of Informatics employs in grades 5-9, in terms of teaching the basics of cybersecurity. So, for example, despite the description of the features of e-mail, fifth graders are not told the basic rules for creating passwords in cyberspace, which will allow them to store personal information in the mail. The article describes the conceptual model of teaching the basics of cybersecurity of primary school students. It implements the idea of continuous learning of cybersecurity, will provide metasubject learning outcomes, will reveal the existing cyberthreats and rules of action at a meeting with them. One of the forms of implementation of the model is cybersecurity week. During the week, it is planned to hold class hours in the format of popular science lectures, interactive games, a contest for the best essay on the topic that reveals the features of cybersecurity, a drawing contest that will reveal the creative potential of children and will reflect their ideas about cyberspace, parent meetings, the theme of which is "Cybersecurity", a contest of tasks on cybersecurity.

Keywords: cybersecurity, schoolchildren, cyberthreat, a conceptual model, cybersecurity week.

Развитие информационных и коммуникационных технологий привело к тому, что сегодня практически каждый человек становится активным пользователем Интернета и, как следствие, уязвимым в плане потери личных данных. Особое беспокойство вызывают школьники, которые, не задумываясь, используют возможности Интернета в своей

повседневной жизни. При этом они не придают значения тому, что есть интернет-преступники, которые совершают мошеннические действия. Как показал проведенный нами опрос 210 учащихся 5-9 классов, только 33 человека из всех опрошенных знают, что такое кибербуллинг, 56 человек могут описать виды интернет-мошенничества, 102 человека смогли сформулировать правила составления надёжных паролей. На сегодняшний день существует множество разработок, направленных на обучение юного поколения правилам корректного поведения в процессе деятельности в Глобальной сети. Однако они не представляют собой целостную систему, которая позволит обучить школьников основам кибербезопасности в основной и старшей школе.

Цель исследования

Цель исследования состоит в создании концептуальной модели обучения основам кибербезопасности учащихся 5-9 классов.

Для достижения данной цели необходимо решить следующие задачи: 1) провести анализ понятия кибербезопасности в нормативных документах, 2) на основе анализа существующего опыта определить цели, задачи и средства обучения основам кибербезопасности в процессе учебной и внеучебной деятельности учащихся 5-9 классов, 3) представить модель обучения основам кибербезопасности в основной школе.

При решении поставленных задач были использованы такие методы исследования, как анализ нормативной документации, психолого-педагогической, учебно-методической литературы по вопросам кибербезопасности, теоретическое моделирование обучения основам кибербезопасности учащихся основной школы, анкетирование с целью сбора эмпирических данных.

Теоретический анализ

Сегодня весь мир охвачен информационным пространством, которое носит название Глобальная сеть или Интернет. Повсеместное его применение, активное расширение области информационных и коммуникационных технологий привело к возникновению проблем, связанных с безопасностью использования компьютеров, смежного оборудования, к введению понятий «информационная безопасность» и «кибербезопасность». Анализ определений данных понятий, представленных в [1] и [2], позволяет говорить о том, что кибербезопасность - это составляющая информационной безопасности, изучающая особенности киберобъектов, источники киберопасности, нормативную документацию, позволяющую обеспечить правовую защиту от возможных источников киберопасности.

Современные дети практически каждый день встречаются и с киберобъектами, и с киберопасностью, так как значительную часть своей жизни «проводят в Интернете». Они используют его возможности при подготовке школьных домашних заданий, смотрят

фильмы, играют в онлайн-игры, общаются в социальных сетях. Поэтому взрослые (учителя, родители, наставники) должны научить их грамотному поведению в киберпространстве. Это подчеркивается и в проекте «Концепции стратегии кибербезопасности Российской Федерации», в которой указано, что сегодня необходимо не только обеспечить разработку и внедрение в образовательный процесс специального курса по информационной безопасности, который включает модули по кибербезопасности, но и «формирование и развитие культуры безопасного поведения в киберпространстве и безопасного использования его сервисов» [3].

Разработчики программного обеспечения, образовательных порталов, школьные учителя предлагают своё видение особенностей обучения основам кибербезопасности. Так, например, академия Яндекса позиционирует курс «Безопасность в интернете», «Лаборатория Касперского» опубликовала на своем сайте советы по кибербезопасности для всех возрастов, в рамках программы Совета Европы «Строим Европу для детей и вместе с детьми» создана игра «Прогулка через Дикий Интернет-лес» (Through the Wild Web Woods) [4]. Учителя школ разрабатывают интегрированные уроки, например, «ОБЖ в сети Интернет» Н.В. Караваевой для школьников 6 класса создан с целью изучения основных правил безопасности при использовании сети Интернет учащимися [5].

Сегодня обучение информатике осуществляется во многих школах начиная с 5 класса. Многие учителя в своей работе используют авторскую программу Л.Л. Босовой. В учебниках для основной школы раскрывается часть вопросов кибербезопасности. Например, в 5 классе представлены темы «Электронная почта. Работаем с электронной почтой» и «Поиск информации», в 7 классе - «Компьютерные сети» и «Правовые нормы использования программного обеспечения». Однако подробный анализ позволил выявить ряд недостатков авторской программы в аспекте обучения основам кибербезопасности:

1) вопросы раскрываются без описания существующих киберугроз и правил действий при встрече с ними. Например, в 5 классе в параграфе 6 представлен материал по теме «Электронная почта». Авторы предлагают описание понятия «электронная почта», особенности строения адреса, однако они не указывают, что нельзя открывать письма от неизвестных отправителей, так как эти письма могут содержать во вложении файлы-вирусы, способные повредить информацию на компьютере или нелегально её использовать. Для ученика 5 класса лучшим выходом из такой ситуации станет обращение к родителям или самостоятельное удаление данного письма. Алгоритм последнего действия достаточно прост, доступен для понимания и осуществления пятиклассником. При выполнении компьютерного практикума (работа 4) пятиклассники учатся регистрировать почтовый ящик, входить в свой почтовый ящик, получать, писать и отправлять электронные письма. При

создании пароля для своего почтового ящика школьникам просто предлагается продумать его варианты. К сожалению, авторы не указывают основные правила создания паролей в киберпространстве, предполагающие применение строчных, прописных, цифровых и специальных символов, а также необходимость периодического изменения пароля с целью сохранения личной информации, хранящейся на почте;

2) изложение материала по кибербезопасности отсутствует в 6 и в 8 классе, то есть в том возрастном периоде, когда у школьников проявляется активный интерес к социальным сетям, а в школе увеличивается количество изучаемых предметов. Как следствие, у детей всё чаще возникает необходимость поиска информации в Глобальной сети при подготовке к урокам;

3) остаются нерассмотренными такие вопросы, как киберпространство, виды киберпреступлений, особенности поведения в ситуациях встречи с киберугрозой, персональные данные и важность их сохранения, законодательство, действующее в Глобальной сети, и т.д.

Предлагаемая концептуальная модель обучения основам кибербезопасности

В основу разработанной нами концептуальной модели обучения основам кибербезопасности положена классификация существующих киберугроз. Большинство современных школьников, их родителей и учителей сталкиваются с теми или иными киберугрозами в своей повседневной жизни, это необходимо учитывать в процессе обучения. В соответствии с вышесказанным была сформулирована цель обучения основам кибербезопасности в школе, которая состоит в том, чтобы сформировать у детей понимание структуры киберпространства, принципов работы в нём, существующих угроз пользователям Интернета, знание правил, которые позволят обеспечить школьникам защиту своих личных данных в Глобальной сети. Поставленная цель может быть достигнута за счет решения следующих задач: 1) ввести основные понятия кибербезопасности, например через использование инструкций, описывающих правила поведения в киберпространстве; 2) сформировать у учащихся умения действовать в киберпространстве с применением на уроках информатики системы прикладных задач; 3) сформировать у учащихся навыки поведения в ситуациях встречи с киберугрозой путем проведения интерактивных игр или применения симуляторов; 4) создать родителям кибербезопасную среду дома с применением учебно-методических материалов для проведения родительских собраний. Одной из возможных организационных форм, позволяющих решить эти задачи, по нашему мнению, является неделя кибербезопасности. В соответствии с выделенными киберугрозами, поставленными целью и задачами, с учетом потребностей участников образовательного процесса, а также на основе методических рекомендаций «Основы кибербезопасности»

определено содержание обучения. Ниже представлена схема предлагаемой нами концептуальной модели обучения основам кибербезопасности (рис. 1).

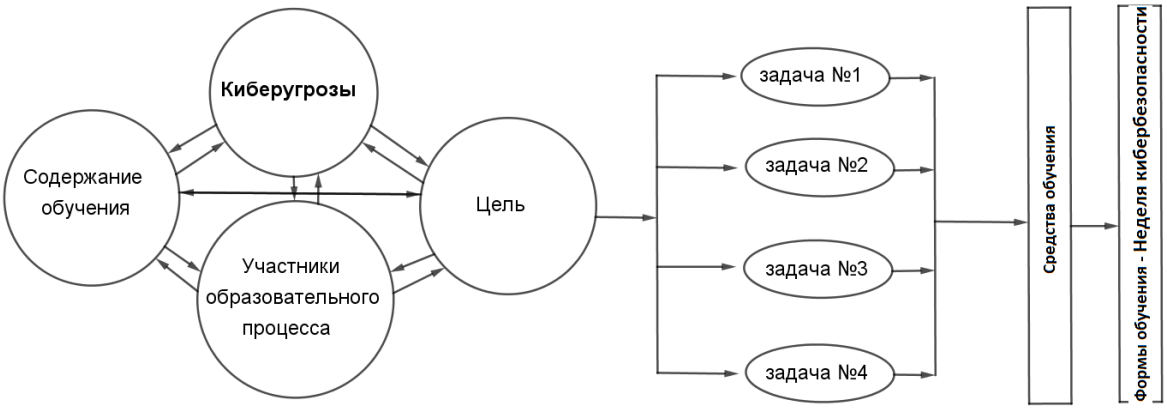

Рис. 1. Концептуальная модель обучения основам кибербезопасности

В рамках описанной модели мы предлагаем:

1) дополнить материал учебников и рабочих тетрадей, входящих в учебно-методический комплект авторской программы Л.Л. Босовой, специально разработанным задачным и теоретическим материалом по вопросам кибербезопасности, который учителя смогут включить в систему учебных занятий, 2) использовать резервные часы на изучение данного раздела, 3) проводить недели кибербезопасности в каждой образовательной организации.

Предлагаемые нами задачи носят прикладной характер. Они составлены с учетом психолого-педагогических особенностей учащихся разных возрастных периодов. Главная их специфика состоит в том, что школьникам приходится принимать решения в задачных ситуациях встречи с киберугрозой. Например, в 5 классе при изучении особенностей поиска информации в Интернете учащимся может быть предложена следующая задача: «В некотором царстве - некотором государстве жил был Царь. Был он жаден и крайне любопытен. Хотелось ему знать всё и обо всём. Хитрый Волшебник решил воспользоваться этой слабостью Царя, чтобы завладеть царством. Подарил он Царю компьютер. Да не простой, а с доступом в Интернет. Обрадовался Царь, зашёл в поисковую систему и начал задавать вопросы: «Какая гора самая высокая?», «Где живут тюлени?», «Как стать ещё богаче?». В ответ на последний вопрос система предложила Царю перевести всю царскую казну в надежный банк с обещанием вернуть через день в два раза больше денег. Царь обрадовался и нажал на кнопку «Перевести». Каково было его удивление, когда в назначенный день он обнаружил абсолютно пустую казну! Как ты думаешь, что произошло с царской казной? Правильно ли поступил Царь? Почему? Что ты можешь ему посоветовать в такой ситуации?». Решая задачу, дети придут к пониманию того, что далеко не всем сайтам

можно доверять. Существуют фишинговые сайты (сайты-двойники), интерфейс которых схож с сайтами известных фирм, банков, интернет-магазинов. Однако обращение к ним опасно и может привести, например, к потере личных данных или финансовых средств.

В 6 классе, по нашему мнению, необходимо дополнить материал учебника не только задачным, но и теоретическим материалом. Например, при изучении параграфа 5 «Системы объектов» учебника [6] учитель в качестве примера смешанных систем может рассмотреть киберпространство. Именно оно содержит в себе материальные (различного вида кабель, компьютеры, устройства для передачи информации, например Wi-Fi-роутер) и нематериальные компоненты (программы, виртуальные деньги, виртуальные преступления). Знакомство с различными исполнителями (параграф 15 «Исполнители вокруг нас») может сопровождаться рассмотрением антивирусных программ как формальных исполнителей. Их действия всегда осуществляются по заранее заданному алгоритму и приводят к одному и тому же результату: компьютер будет очищен от вредоносного программного обеспечения. Вопросы и задания после параграфа 16 «Формы записи алгоритмов» мы рекомендуем дополнить задачей на составление алгоритма создания безопасного профиля в социальной сети.

Каждый год в школах проводятся предметные недели. Мы предлагаем ежегодно проводить неделю кибербезопасности. Во время классных часов для учащихся с 5 по 11 класс учителя проведут различные мероприятия, цель которых состоит в том, чтобы сформировать и/или развить представления школьников о кибербезопасности, особенностях поведения в ситуациях встречи с киберугрозой и т.д. Классный час в виде научно-популярной лекции с применением интерактивных игр, составленных в формате известной игры «Своя игра», позволит заинтересовать учащихся, привлечь их внимание к существующим в киберпространстве проблемам. Учителя русского языка могут присоединиться и провести конкурс на лучшее сочинение по теме, раскрывающей особенности кибербезопасности. Конкурс рисунков для учащихся основной школы позволит раскрыть творческий потенциал детей и отразить их представления о киберпространстве. Привлечение родителей к данной проблематике может осуществляться путем проведения родительских собраний, главная тема которых «Кибербезопасность». В содержание собрания мы предлагаем включить изучение законодательных актов в области кибербезопасности, особенностей применения антивирусного программного обеспечения, программ-фильтров. Обязательным является ознакомление родителей с так называемыми необычными онлайн-играми, существующими «группами смерти». Задача классного руководителя будет состоять и в том, чтобы раскрыть поведенческие особенности детей, попавших под влияние таких организаций. Полученные знания позволят родителям защитить своих детей от киберугроз и

научить их противостоять этим явлениям киберпространства. Учителя и администрация школ организуют круглые столы, на которых смогут обсудить процесс и итоги проведения недели кибербезопасности, составить дальнейший план действий в данном направлении.

Обязательной составляющей недели кибербезопасности должен стать «Конкурс по кибербезопасности» на базе кафедры экспериментальной математики и информатизации образования САФУ имени М.В. Ломоносова. Впервые массово он будет проведен в ноябре 2018 года. Его участниками станут учащиеся 5-9 классов школ Архангельской области. Весь задачный материал разработан студентами 4 и 5 курсов направления подготовки 44.03.05 «Педагогическое образование» под руководством преподавателей кафедры. В основе создания задач лежали методические рекомендации «Основы кибербезопасности» и авторская программа Л.Л. Босовой.

Полученные результаты

Таким образом, мы разработали концептуальную модель обучения основам кибербезопасности учащихся основной школы. Она предполагает такую организацию учебного процесса, которая в полной мере позволит реализовать идею непрерывного обучения кибербезопасности, обеспечить метапредметность результатов обучения, раскрыть существующие сегодня киберугрозы и правила действий при встрече с ними. Экспериментальная апробация началась ещё в 2016 году. Описанная в [7] идея создания курса «Основы информационной безопасности» для родителей учащихся общеобразовательной школы реализована в ряде школ Архангельской области. В годовой план родительских собраний были включены занятия по темам «Ребенок и Интернет: За и против», «Насилие в Интернете: как распознать, к кому обратиться», «Безопасные электронные ресурсы для ребенка (Позитивный контент)» и т.д., всего 10 часов.

Результаты проведенного анкетирования родителей школьников (290 человек) показали, что по завершении обучающих мероприятий по кибербезопасности у большинства сформировались знания и умения в этой области. Так, например, знают различные виды киберугроз 273 человека, ранее – 65 (вопрос 1). При ответе на вопрос о том, обсуждалась ли с детьми модель поведения в ситуациях встречи с киберугрозами, утвердительно ответили 281 человек, ранее – 13 (вопрос 2). Значительно выросли показатели и при ответах на другие вопросы: установлены ли программы-фильтры на домашнем компьютере (вопрос 3), установлены ли детские поисковые системы на домашнем компьютере (вопрос 4) и пр. На рисунке 2 представлена диаграмма с результатами двух анкетирований на примере вопросов 1-4.

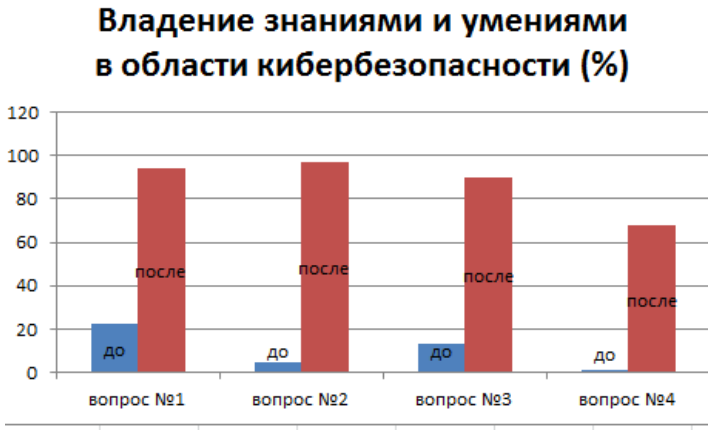

Рис. 2. Результаты анкетирования родителей учащихся

Заключение

В процессе проводимого исследования было установлено, что все участники образовательного процесса должны быть компетентны в области кибербезопасности. Наилучший эффект будет достигнут при условии комплексного подхода к решению данной задачи. Мы считаем, что он подразумевает ежегодное проведение в образовательных организациях недель кибербезопасности, систематическое использование учителями в процессе обучения информатике сборника, содержащего теоретический и задачный материал по вопросам кибербезопасности и дополняющего учебно-методический комплект Л.Л. Босовой.

Список литературы

1. Указ Президента РФ от 5 декабря 2016 г. № 646 “Об утверждении Доктрины информационной безопасности Российской Федерации” [Электронный ресурс]. URL: http://www.garant.ru/products/ipo/prime/doc/71456224 (дата обращения: 01.09.2018).

2. Марков А.С., Цирлов В.Л. Руководящие указания по кибербезопасности в контексте ISO 27032 [Электронный ресурс]. URL: http://cyberrus.com/wp-content/uploads/2014/03/28-35.pdf (дата обращения: 01.09.2018).

3. Концепция стратегии кибербезопасности Российской Федерации. Проект [Электронный ресурс]. URL: http://council.gov.ru/media/files/41d4b3dfbdb25cea8a73.pdf (дата обращения: 02.06.2018).

4. Wild Web Woods [Электронный ресурс]. URL: http://www.wildwebwoods.org/popup.php?lang=ru (дата обращения: 07.09.2018).

5. Караваева Н.В. Безопасность в сети Интернет [Электронный ресурс]. URL: http://www.59428s002.edusite.ru/ (дата обращения: 10.09.2018).

6. Босова Л.Л., Босова А.Ю. Информатика: учебник для 6 класса М.: БИНОМ. Лаборатория знаний, 2013. 213 с.
7. Троицкая О.Н., Попов А.В. О необходимости разработки курса «Основы информационной безопасности» для родителей учащихся общеобразовательной школы [Электронный ресурс]. URL: http://news.scienceland.ru/2016/02/14/1085/ (дата обращения: 11.08.2018).