О. Н. Троицкая, О. Л. Безумова, Т. С. Ширикова,
Северный (Арктический) федеральный университет имени М. В. Ломоносова, г. Архангельск

ОСОБЕННОСТИ ОРГАНИЗАЦИИ И ПРОВЕДЕНИЯ КОНКУРСА ЗАДАЧ ПО КИБЕРБЕЗОПАСНОСТИ

Аннотация

Подготовка учащихся к безопасному поведению в сети Интернет — одна из важнейших задач общеобразовательной школы, признанная на государственном уровне, что подтверждается утверждением распоряжением Правительства РФ от 2 декабря 2015 года Концепции информационной безопасности детей на 2018–2020 годы, а также изданием 27 февраля 2018 года приказа Минкомсвязи России «Об утверждении плана мероприятий по реализации Концепции информационной безопасности детей на 2018–2020 годы». В рамках реализации этого плана в октябре 2018 года в Архангельской области прошла Первая областная неделя кибербезопасности. Статья посвящена описанию одного из мероприятий этой недели — конкурса задач по кибербезопасности. Представлены концептуальные основы разработки системы конкурсных заданий, предложенных учащимся разных классов основной школы, приведены примеры задач с решениями. Авторы статьи полагают, что включение подобных задач в содержание школьных учебников информатики даст учителям действительно эффективные инструменты для подготовки учащихся к распознаванию киберугроз и правильному поведению при встрече с ними.

Ключевые слова: кибербезопасность, киберугроза, уровни готовности, конкурс задач по кибербезопасности.

DOI: 10.32517/2221-1993-2019-18-6-5-9

1. Введение

Проникновение интернета во все сферы жизнедеятельности современного общества привело к вовлечению в информационное пространство и подрастающего поколения. Родители, покупая своим детям компьютеры и мобильные компьютерные устройства, далеко не всегда задумываются над тем, с какими опасностями могут встретиться их дети в киберпространстве. На территории школы эти угрозы минимизированы ограничением доступа обучающихся к видам информации, распространяемой по сети Интернет, причиняющей вред их здоровью или развитию и не соответствующей задачам образования [5]. За стенами школы дети оказываются один на один с этими угрозами.

Сколько времени ученики основной школы проводят в сети Интернет? Чем привлекает их киберпространство? Ответы на эти вопросы авторы статьи попытались получить, проведя **опрос учащихся одной из школ города Архангельска**. В опросе приняли участие 320 школьников VII—IX классов. Результаты показали, что среднее время, которое они проводят в интернете, составляет от полутора до четырех часов. Это время дети тратят на выполнение домашних заданий, просмотр фильмов, онлайн-игры, общение в социальных сетях. При этом 72 % опрошенных отметили, что встречались

Контактная информация

Троицкая Ольга Николаевна, канд. пед. наук, доцент, зав. кафедрой экспериментальной математики и информатизации образования, Высшая школа информационных технологий и автоматизированных систем, Северный (Арктический) федеральный университет имени М. В. Ломоносова, г. Архангельск; *адрес:* 163002, г. Архангельск, набережная Северной Двины, д. 17; *e-mail:* o.troitskaya@narfu.ru

Безумова Ольга Леонидовна, канд. пед. наук, доцент, доцент кафедры экспериментальной математики и информатизации образования, Высшая школа информационных технологий и автоматизированных систем, Северный (Арктический) федеральный университет имени М. В. Ломоносова, г. Архангельск; *адрес:* 163002, г. Архангельск, набережная Северной Двины, д. 17; *e-mail:* o.bezumova@narfu.ru

Ширикова Татьяна Сергеевна, канд. пед. наук, доцент кафедры экспериментальной математики и информатизации образования, Высшая школа информационных технологий и автоматизированных систем, Северный (Арктический) федеральный университет имени М. В. Ломоносова, г. Архангельск; *адрес:* 163002, г. Архангельск, набережная Северной Двины, д. 17; *e-mail:* t.shirikova@narfu.ru

O. N. Troitskaya, O. L. Bezumova, T. S. Shirikova,
Northern (Arctic) Federal University named after M. V. Lomonosov, Arkhangelsk

FEATURES OF THE ORGANIZATION AND CONDUCT OF THE CONTEST OF TASKS ON CYBERSECURITY

Abstract

Preparing children for safe behavior on the Internet is one of the most important tasks of secondary school, which is recognized at the state level. It is confirmed by the order of the Government of the Russian Federation of December 2, 2015 "Concept of Information Security of Children for 2018–2020" and the order of the Ministry of Digital Development, Communications and Mass Media of the Russian Federation of February 27, 2018 "On Approval of the Action Plan for the Implementation of the Concept of Information Security of Children for 2018–2020". The First Region Week of Cybersecurity was held as part of the implementation of this plan in October 2018 in the Arkhangelsk region. The article is devoted to the description of one of the events of this week — the contest of tasks on cybersecurity. The article presents the conceptual basis for the development of a system of competitive tasks, which were offered to schoolchildren of different classes of secondary school, and provides examples of problems with solutions. The authors of the article believe that the inclusion of such tasks in the content of school computer science textbooks will give teachers really effective tools to prepare schoolchildren for recognizing cyberthreats and the correct behavior when meeting with them.

Keywords: cybersecurity, cyberthreat, levels of readiness, the contest of tasks on cybersecurity.

с негативной, неприятной и даже опасной информацией в сети. К такой информации школьники отнесли навязчивую рекламу, приглашение стать участником «необычной» группы, предложение больших скидок в обмен на сообщение личных данных (номер мобильного телефона, логин и пароль для входа в социальную сеть и т. д.), приглашение встретиться в реальной жизни с новыми интернет-знакомыми. Дети указали, что испытали чувство дискомфорта и даже страха в некоторых ситуациях, но далеко не все из них обращались за помощью к родителям и друзьям.

Раскрыть перед учащимися спектр возможных рисков киберпространства, научить их правильному поведению при встрече с киберугрозой — это задача, реализация которой сегодня возложена на общеобразовательную школу. Для оказания помощи школам в решении данной задачи были разработаны **методические рекомендации по включению в учебные планы общеобразовательных школ курса «Основы кибербезопасности»** и модернизации учебных программ уже существующих предметов под задачи обучения учащихся безопасному поведению в сети Интернет [3]. Главная цель данного курса состоит в том, чтобы дать учащимся общие представления о безопасности в информационном обществе, на этой основе сформировать у обучающихся понимание технологий информационной безопасности и умения применять правила кибербезопасности во всех сферах деятельности. Содержание курса представлено модулями, раскрывающими способы борьбы с тем или иным видом киберугроз: «Проблемы интернет-зависимости», «Мошеннические действия в интернете. Киберпреступления», «Правовые аспекты защиты киберпространства» и др. Кроме перечня модулей и требований к результатам их освоения в методических рекомендациях представлены примеры учебных занятий, отнесенных к разным предметам и ориентированных на решение задач обучения учащихся кибербезопасности.

Анализ указанных материалов, а также разработок, предлагаемых самими учителями [1, 2 и др.], свидетельствует о том, что ведущим средством формирования навыков безопасного поведения в киберпространстве остаются *материалы инструктивного характера*.

Понимая недостаточность подобного подхода, авторы статьи предлагают дополнить такие материалы *ситуационными задачами* на распознавание киберугроз и принятие правильных решений при встрече с ними. Именно такие задачи и предлагались участникам конкурса, проведенного в Архангельской области в рамках Первой областной недели кибербезопасности в октябре 2018 года.

2. Теоретические основы разработки задач по кибербезопасности

За основу разработки содержания задач были взяты тематические модули методических рекомендаций «Основы кибербезопасности» [3]. С учетом возрастных особенностей, интересов и деятельности учащихся в киберпространстве данные модули были детализированы.

Так, в рамках модуля «Общие сведения о безопасности ПК и интернета»:

- в V классе рассматривались компьютерные игры (бесплатные и платные) и особенности осуществления покупок в интернете;
- в VI классе внимание было уделено вопросам киберугроз для мобильных устройств;
- задания в VII классе были направлены на раскрытие особенностей защиты персональных данных;
- в VIII и IX классах задания включали учащихся в деятельность по раскрытию киберпреступлений, их предотвращению и в борьбу с ними.

Приведем примеры задач, проверяющих владение содержанием модуля «Общие сведения о безопасности ПК и интернета» курса «Основы кибербезопасности» у учащихся разного возраста.

Задача 1 (V класс).

Инструкция.

Выберите из предложенных несколько верных вариантов ответа.

Задание.

Разработчик игры Stoon потратил пять лет на ее создание. Когда Stoon вышел в прокат, мальчик Леня очень захотел приобрести эту игру. Придя в магазин, он обнаружил, что у игры высокая стоимость, поэтому решил обратиться в интернет за помощью. В сети, перейдя по первой ссылке, Леня увидел надпись: «Игра Stoon бесплатная и скачать ее можно по ссылке, данной ниже».

Из представленных ниже вариантов выберите тот, который вы предложили бы Лене.

а) Скачать игру с данного сайта, так как там она бесплатная.

б) Попросить денег у родителей и купить игру в магазине.

в) Продолжить искать игру в интернете с возможностью купить ее со скидкой.

Правильные ответы: б и *в*.

Задача 2 (VI класс).

Инструкция.

Прочитайте описание ситуации и дайте развернутые ответы на поставленные вопросы.

Задание.

Мама Кати, придя на работу, обнаружила, что забыла дома свой мобильный телефон. С рабочего телефона она позвонила Кате с просьбой принести ей мобильник на работу. Закончив разговор, Катя услышала, что в соседней комнате на мамин мобильный телефон пришло SMS-сообщение. Так как у Кати с мамой были доверительные отношения, девочка прочитала полученное SMS-сообщение. Катя заметила, что сообщение пришло от неизвестного отправителя. Оно содержало следующий текст: «Доброго времени суток! По вашим паспортным данным найдены страховые начисления в размере 47 руб. Подробности на сайте: http://snils-gost.online». Девочка, не задумываясь о последствиях, перешла по ссылке. В открывшемся окне браузера не было никакой информации о паспортных данных мамы, и Катя закрыла это окно. Через пару минут на мобильный телефон пришло SMS-сообщение от сотового оператора: «Ваш баланс менее 5 рублей». Заподозрив, что исчезновение средств

связано с переходом по ссылке из SMS-сообщения, Катя испугалась и побежала на работу к маме.

а) Какие ошибки допустила Катя?

б) Какие последствия могут возникнуть в результате действий Кати? Обоснуйте свой ответ.

в) Составьте рекомендацию для детей, в которой будет содержаться описание признаков SMS-мошенничества и правил поведения при встрече с ним.

Правильные ответы:

а) Прочитала сообщение, адресованное не ей; перешла по подозрительной ссылке.

б) Переход по ссылке может привести к тому, что:

- произойдет списание денег со счета;
- в телефон будут загружены вирусы, которые прекратят нормальную работу устройства и скачают все персональные данные;
- при подключении телефона к компьютеру произойдет заражение и этого устройства.

в) *Признаки SMS-мошенничества*:

- номер от неизвестного отправителя;
- номер очень короткий;
- в сообщении содержится информация о выигрыше, для получения которого необходимо перейти по указанной ссылке;
- требование обратного звонка;
- просьба о помощи, связанной с переводом денег.

Правила поведения:

- никогда не перезванивать и не переводить деньги;
- удалить SMS-сообщение;
- перезвонить своему мобильному оператору для решения «проблемы»;
- установить на телефон антивирусную программу.

Задача 3 (VII класс).

Инструкция.

Дайте краткий ответ.

Задание.

Вам на электронную почту пришло письмо следующего содержания: «Для подтверждения того, что вы являетесь настоящим пользователем ВКонтакте, перейдите по ссылке https://vvk.com/id47073790». Стоит ли переходить по ссылке и почему? Обоснуйте свой ответ.

Правильный ответ.

Переходить по ссылке нельзя. Данный адрес не является официальным адресом сайта социальной сети «ВКонтакте», так как в адресе имеется лишняя буква v — vvk.com. Если при переходе по этой ссылке ввести свой логин и пароль, то мошенник получит доступ к вашим персональным данным.

Задача 4 (VIII класс).

Инструкция.

Прочитайте описание ситуации и дайте развернутые ответы на поставленные вопросы.

Задание.

Гуляя по торговому центру, Таня увидела платье, которое ей очень понравилось, но оно было дорогим. Девочка решила проверить, сколько это платье стоит в интернет-магазине. Не задумываясь, она подключилась к одной из обнаруженных открытых сетей FreeWiFi. Зайдя на сайт интернет-магазина, девочка обнаружила точно такое же платье ее размера, но по цене в три раза дешевле. Обрадовавшись, Таня оформила онлайн-покупку, введя номер банковской карты и трехзначный код, указанный на обратной стороне карты. После этого она авторизовалась в социальной сети и своей радостной новостью поделилась с подружкой.

а) Какие ошибки совершила Таня?

б) Какие негативные последствия совершенного ею поступка могут возникнуть? Обоснуйте свой ответ.

в) Сформулируйте правила, которыми нужно руководствоваться при использовании общественной Wi-Fi сети.

Правильные ответы.

а) Подключившись к общественной Wi-Fi сети, Таня передала конфиденциальные данные: ввела номер и код с банковской карты, авторизовалась в социальной сети — ввела логин и пароль.

б) Негативные последствия совершенного поступка: злоумышленники с применением введенных Таней логина и пароля могут взломать ее страницу в социальной сети, тем самым узнать личную информацию, от лица Тани просить у «друзей» деньги, шантажировать саму Таню и т. д. Кроме того, так как при оплате покупки Таня ввела трехзначный код с карты, то теперь ее картой могут воспользоваться мошенники, оплачивая свои покупки в интернете.

в) *Правила:*

- не доверять сетям с подозрительными названиями (FreeInternet или FreeWiFi);
- не совершать онлайн-покупки и банковские переводы в общественных сетях;
- не передавать конфиденциальную информацию;
- не вводить логины и пароли от различных сайтов при использовании общественной Wi-Fi сети.

Задача 5 (IX класс).

Инструкция.

Прочитайте описание ситуации и дайте развернутые ответы на поставленные вопросы.

Задание.

Света (16 лет) рассталась со своим молодым человеком и очень переживала по этому поводу. Для того чтобы разобраться в причинах расставания, девушка начала поиск в интернете информации об отношениях между людьми противоположного пола. На одном из форумов Света прочитала похожую историю. Она написала автору сообщение, тем самым начав переписку с незнакомым человеком. Виртуальный собеседник сообщила о себе, что ее зовут Настя и живет она в том же городе. Они вместе обсуждали произошедшее, делились чувствами и переживаниями. В одном из сообщений Настя написала, что для того, чтобы забыть несчастную любовь, нужно найти увлечение, хобби. Настя предложила Свете встретиться и пойти вместе в студию танцев.

а) Стоит ли Свете согласиться на встречу с Настей? Обоснуйте свой ответ.

б) Какими могут быть негативные последствия встречи Светы и ее виртуального собеседника?

в) Какими способами Света могла бы себя обезопасить?

Правильные ответы.

а) Свете не стоит соглашаться на встречу, так как она не может быть уверена, что виртуальный собеседник действительно является тем, за кого себя выдает.

б) Возможные негативные последствия: вовлекут в религиозные или экстремистские организации, станет жертвой реального преступника.

в) Собираясь на встречу, Света должна обязательно сообщить кому-то из близких, на встречу с кем и куда она пошла, когда выйдет на связь. Встречу назначить в людном и хорошо знакомом месте.

Приведенные примеры показывают, что задачи носили в основном ситуационный характер, т. е. описывали ситуации, с которыми ребята встречались или могли встретиться в жизни. Требования задач формулировались таким образом, чтобы включать учащихся в виды деятельности, отнесенные к разным уровням освоения содержания курса «Основы кибербезопасности».

Уровни определялись в соответствии с таксонометрией уровней освоения знаний В. П. Беспалько: знания-представления, знания-копии, знания-умения, знания-трансформации:

- задачи первого уровня сложности требовали от учащихся правильно распознать наличие и вид киберугрозы;
- задачи второго уровня — выбрать из числа предложенных выходов из ситуации тот, который соответствует описанной киберугрозе;
- задачи третьего уровня — применить в стандартной ситуации освоенные способы действия при встрече с киберугрозой;
- задачи четвертого уровня — принять собственное обоснованное решение в нестандартной ситуации встречи с киберугрозой.

В таблице представлены примеры задач соответствующих уровней, адресованные учащимся V класса.

Таблица

Уровни готовности к принятию обоснованных решений в ситуациях встречи с киберугрозами

<table>
<tr><th>Уровень готовности</th><th>Примеры заданий</th></tr>
<tr><td>I</td><td>Задача 6.
Инструкция.
Запишите слово «да», если утверждение истинное, и слово «нет», если утверждение ложное.
Вирус может попасть в компьютер следующим образом:
а) прослушивание музыки в социальных сетях (да/нет);
б) скачивание файлов со сторонних сайтов (да/нет);
в) работа в программах Microsoft Office (да/нет);
г) переход по подозрительным ссылкам из сообщений от неизвестных отправителей (да/нет);
д) просмотр фильмов, расположенных в памяти компьютера (да/нет).</td></tr>
<tr><td>II</td><td>Задача 7.
Инструкция.
Установите соответствие элементов двух множеств.
<table>
<tr><th>Характеристика интернет-зависимости</th><th>Виды интернет-зависимости</th></tr>
<tr><td>1. Постоянное участие в интернет-аукционах</td><td>А. Игровая</td></tr>
<tr><td>2. Навязчивое увлечение компьютерными играми</td><td>Б. Финансовая</td></tr>
<tr><td>3. Постоянное участие в чатах</td><td>В. Социальная</td></tr>
</table></td></tr>
<tr><td>III</td><td>Задача 8.
Инструкция.
Дайте краткий ответ.
Задание.
Васе на уроке истории задали сделать доклад. Недолго думая, он решил найти готовый вариант в интернете. В поисковой строке мальчик ввел тему доклада и перешел по первой же появившейся ссылке. В окне браузера он увидел яркую кнопку «Скачать» и нажал на нее. Неожиданно компьютер начал перезагрузку, а когда включился, то на рабочем столе исчезли все ярлыки.
Что произошло с компьютером?
Какие действия необходимо предпринять мальчику для выхода из создавшейся ситуации?</td></tr>
<tr><td>IV</td><td>Задача 9.
Инструкция.
Прочитайте описание ситуации и дайте развернутые ответы на поставленные вопросы.
Задание.
В одной из социальных сетей Игорь познакомился с мальчиком Витей. После нескольких дней общения собеседник начал задавать вопросы личного характера: «Где и с кем ты живешь?», «Дай номер своего телефона», «Расскажи про свою семью поподробнее», «Где работают твои родители?», «Твои родители много зарабатывают?» и т. п. Игорь, не задумываясь о последствиях, рассказал собеседнику все про себя и свою семью, а также отправил семейные фотографии. Через какое-то время Игорю на телефон стали приходить сообщения с требованиями перевода денежных средств на указанный счет. При этом ему угрожали, что в случае невыполнения требований информация о родных Игоря попадет в общий доступ в интернете.
а) Составьте список ошибок, которые совершил Игорь.
б) Каким образом можно избежать ситуации, в которой оказался Игорь? Обоснуйте свой ответ.
в) Составьте рекомендацию для детей, которые оказались в похожей ситуации.</td></tr>
</table>

Представленная в таблице задача 6 позволит не только выявить наличие у школьников представлений о таком понятии, как «вирусная программа», но и определить содержащиеся в их субъектном опыте знания о способах распространения вирусных программ.

Задача 7 вовлечет пятиклассников в деятельность по раскрытию содержания понятия «интернет-зависимость». Решение данной задачи основано на осознании школьниками существующих видов интернет-зависимости.

Задача 8 позволит пятиклассникам четко и кратко описать особенности действий в стандартной ситуации заражения компьютера вирусом. Решение, которое могут предложить учащиеся, основано на информации, полученной на уроках информатики и на классном часе, тема которого «Безопасный интернет». Школьники знают признаки заражения компьютерным вирусом и способы борьбы с ним с помощью антивирусных программ.

Содержание задачи 16 многокомпонентно. Оно включает в себя такие аспекты кибербезопасности, как правила общения в интернете, персональные данные, виды киберпреступлений. При этом школьникам представлено описание возможных последствий нарушения данных правил. На уровне явных знаний пятиклассники составят список ошибок, которые совершил герой задания (предоставил неизвестному человеку, который оказался киберпреступником, личную информацию о себе и о своей семье), далее они продумают, как избежать ситуации, в которой оказался герой, и, наконец, выступая в роли эксперта, сами составят рекомендацию для детей, оказавшихся в похожей ситуации.

Для организационной и методической поддержки конкурса задач по кибербезопасности была создана отдельная страница сайта «Неделя кибербезопасности» [4], на которой можно было зарегистрироваться для участия в конкурсе и затем ознакомиться с его результатами (см. рис.).

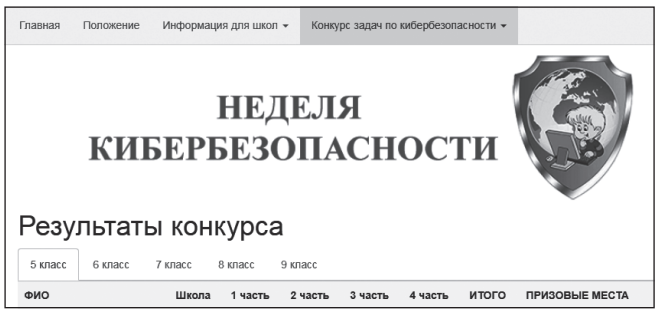

Рис. Страница сайта «Неделя кибербезопасности»

3. Итоги конкурса задач по кибербезопасности

Конкурс задач по кибербезопасности впервые состоялся 27 октября 2018 года на базе Высшей школы информационных технологий и автоматизированных систем Северного (Арктического) федерального университета имени М. В. Ломоносова. Он представлял собой завершающее мероприятие Первой областной недели кибербезопасности. В ее рамках были проведены:

- классные часы «Безопасный интернет»;
- конкурс на лучшее сочинение по теме, раскрывающей особенности кибербезопасности;
- конкурс рисунков, позволяющий раскрыть творческий потенциал детей и отразить их представления о киберпространстве;
- родительские собрания, тема которых — «Кибербезопасность».

Особенность организации и проведения конкурса задач по кибербезопасности состояла в том, что непосредственно составлением заданий занимались студенты, обучающиеся по направлению подготовки 44.03.05 «Педагогическое образование» (с двумя профилями подготовки: «Математика» и «Информатика»).

В конкурсе приняли участие учащиеся V—IX классов школ города Архангельска. Первичный анализ полученных результатов показал, что большинство участвовавших в конкурсе школьников распознают типичные ситуации риска, знают возможные последствия принятия неверного решения, стараются выбирать оптимальную стратегию поведения при встрече с киберугрозой.

4. Выводы

Каждый школьник должен быть компетентен в области кибербезопасности. Он должен не только осознавать угрозы киберпространства, но и уметь принимать правильные решения в ситуациях встречи с киберпреступниками. Как показал наш опыт, именно конкурс задач по кибербезопасности выступает эффективным средством подготовки школьников к безопасному поведению в киберпространстве.

Мы полагаем, что в будущем данный конкурс должен быть дополнен конкурсом на самостоятельное составление школьниками задач по кибербезопасности, что позволит большему количеству учащихся достигнуть четвертого уровня готовности к принятию обоснованных решений в ситуациях встречи с киберугрозами. Мы предполагаем, что этот конкурс будет проходить в два этапа. На первом этапе, который планируется проводить заочно, будут отобраны лучшие работы школьников. В дальнейшем их авторы будут приглашены на второй, очный этап, который состоится на базе Высшей школы информационных технологий и автоматизированных систем Северного (Арктического) федерального университета имени М. В. Ломоносова.

Список использованных источников

1. *Горячева Т. А.* Конспект урока информатики и ИКТ по теме «Безопасный интернет» (9 класс). http://mucro.gorunodubna.ru/wp-content/uploads/2015/11/Sbornik-bezopasnyj-internet.pdf

2. *Караваева Н. В.* Интегрированный урок информатики и ОБЖ для 6 класса по теме «ОБЖ в сети Интернет». http://www.59428s002.edusite.ru/p174aa1.html

3. Методические рекомендации «Основы кибербезопасности». https://www.единыйурок.рф/osnovy

4. Неделя кибербезопасности. http://itprojects.narfu.ru/cybersecurity/

5. Правила подключения общеобразовательных учреждений к единой системе контент-фильтрации доступа к сети Интернет, реализованной Министерством образования и науки Российской Федерации (утв. Министром образования и науки Российской Федерации А. А. Фурсенко 11 мая 2011 года № АФ-12/07вн). http://docs.cntd.ru/document/499053312