УДК [71.14.011.33:004.056]:[371.31:004.771]

Троицкая О. Н., Яворская А. М.

ОБУЧЕНИЕ ОСНОВАМ КИБЕРБЕЗОПАСНОСТИ В РАМКАХ ДИСТАНЦИОННОГО КУРСА ПОВЫШЕНИЯ КВАЛИФИКАЦИИ УЧИТЕЛЕЙ

Ольга Николаевна Троицкая

заведующий кафедрой экспериментальной математики и информатизации образования,

кандидат педагогических наук, доцент,

o.troitskaya@narfu.ru

Высшая школа информационных технологий и автоматизированных систем, ФГАОУ ВО «Северный (Арктический) федеральный университет имени М. В. Ломоносова», Россия, Архангельск,

Анна Михайловна Яворская

студент

anya.kolosova222@gmail.com

Высшая школа информационных технологий и автоматизированных систем, ФГАОУ ВО «Северный (Арктический) федеральный университет имени М. В. Ломоносова», Россия, Архангельск,

TEACHING THE BASICS OF CYBERSECURITY AS PART OF A DISTANCE LEARNING COURSE FOR TEACHERS

Troitskaya Olga Nikolaevna

Federal State Autonomous Educational Institution of Higher Education «Northern (Arctic) Federal University named after M.V. Lomonosov»

Anna Mikhailovna Yavorskaya

Federal State Autonomous Educational Institution of Higher Education «Northern (Arctic) Federal University named after M.V. Lomonosov»

Аннотация: *В статье обоснована необходимость обучения учителей основам кибербезопасности в рамках дистанционного курса повышения квалификации. Определены особенности проектирования содержания обучения данного курса, приведены примеры применяемых контекстных задач.*

Abstract*: The article substantiates the need to teach teachers the basics of cybersecurity in the framework of a distance learning course. The features of designing the content of the training of this course are determined, examples of applied contextual tasks are given.*

Ключевые слова: *педагог, процесс обучения, кибербезопасность, повышение квалификации, методика обучения.*

Keywords: *teacher, learning process, cybersecurity, advanced training, teaching methods.*

Вопросы обеспечения информационной безопасности (ИБ) детей являются сегодня обсуждаемыми не только специалистами в сфере IT-технологий, но учителями и родителями. Обеспокоенность вызывают участившиеся случаи совершения киберпреступлений в адрес детей. Правительство с целью нивелирования киберугроз на законодательном уровне утвердило ряд документов и нормативно-правовых актов (таблица 1).

Таблица 1 — Нормативно-правовые документы в области ИБ детей

Год утверждения	**Название документа**	**Содержание**
24.07.1998	Федеральный закон № 124-ФЗ «Об основных гарантиях прав ребенка в Российской Федерации» [5]	Устанавливает основные гарантии прав и законных интересов ребенка, предусмотренных Конституцией РФ, в целях создания правовых, социально-экономических условий для реализации прав и законных интересов ребенка, а также ИБ детей. Государство признает детство значимым этапом жизни любого ребёнка и исходит из принципов приоритетности подготовки детей к реальной жизни в обществе, становления у них общественно важной и творческой активности, воспитания в них высоких моральных качеств, патриотизма и гражданственности.

29.12.2010	Федеральный закон № 436 «О защите детей от информации, причиняющей вред их здоровью и развитию» [4]	Контролирует взаимоотношение, связанные с защитой детей от калечащего их психику коммуникационного влияния, жестокости и насилия в доступных СМИ. В Законе дано определение понятию ИБ детей — «состояние защищенности детей, при котором отсутствует риск, связанный с причинением информацией вреда их здоровью и (или) физическому, психическому, духовному, нравственному развитию» [4].
02.12.2015	Концепция информационной безопасности детей [1]	Описаны основные принципы обеспечения ИБ детей. Выделены механизмы реализации и определены приоритетные задачи государственной политики в области ИБ детей.
05.12.2016	Указ Президента РФ № 646 «Об утверждении Доктрины информационной безопасности Российской Федерации» [2]	Указаны основные способы обеспечения ИБ в области науки, технологий и образования и определены основные угрозы ИБ. Доказана необходимость в процессе формирования новых знаний в области обеспечения ИБ кадровых возможностей.

Данная политика нашла своё продолжение в разработке методических рекомендаций «Основы кибербезопасности» [2], которые были одобрены на парламентских слушаниях «Актуальные вопросы обеспечения безопасности и развития детей в информационном пространстве» [3] в Совете Федераций в апреле 2017 года. Авторы методических рекомендаций подчеркивают необходимость формирования навыков безопасной работы учащихся в киберпространстве на протяжении всего обучения в школе (со 2 по 11 класс) путём включения вопросов теории кибербезопасности в различные школьные предметы (обществознание, информатика, ОБЖ и др.). Таким образом, можно говорить не только о метапредметном характере данной области научного знания, но и о соответствующем уровне компетентности педагогов в данной сфере. Следовательно, сегодня требуется обеспечить повышение квалификации учителей в области теории и методики обучения кибербезопасности вне зависимости преподаваемых ими дисциплин.

Проведённый анализ центров дополнительного образования (Kaspersky.academy, Московский центра дистанционного образования «Бакалавр-Магистр», Единый урок и другие), говорит о том, что все предлагаемые курсы адресованы ИТ-специалистам (будущим и действующим). Вопросы методики преподавания основ кибербезопасности остаются полностью нераскрытыми. Именно поэтому мы предлагаем курс «Обучение основам кибербезопасности в образовательных организациях» с применением дистанционных образовательных технологий. Мы полагаем, что основной целью курса является формирование готовности учителей школ к обучению учащихся основам кибербезопасности. В соответствии с целью мы выделили следующие задачи курса:

- изучить теорию кибербезопасности в образовательном аспекте,
- повысить уровень сформированности умений и навыков в области кибербезопасности учителей школ,
- раскрыть методические особенности обучения учащихся школ основам кибербезопасности,
- сформировать педагогический опыт обучения основам кибербезопасности.

Процесс проектирования содержания обучения в рамках данного курса представлен на рисунке 1.

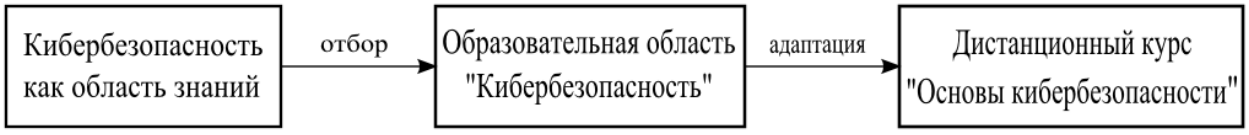


Рисунок 1 — Процесс проектирования содержания курса

В рамках данного курса предусмотрено изучение четырех тем (таблица 2).

Таблица 2 — Содержание тем курса

Тема курса	Содержание
Нормативная документация в области кибербезопасности	Рассматриваются законодательные акты в области кибербезопасности. Вводятся такие понятия как собственность в Интернете, авторское право, интеллектуальная собственность. Указывается ответственность за интернет-мошенничество. Разбор технологии анализа цифрового следа.
Виды киберпреступлений, способы и методы защиты от них	Описывает все аспекты ИБ, которая включает в себя анализ теоретических и практических рисков. Описана классификация киберпреступлений и виды киберугроз. Разбор и анализ конкретных ситуаций и примеров по данной теме.
Формирование поведенческих навыков безопасной работы в киберпространстве	Описаны особенности общения детей в сети и выявлены его последствия. Рассмотрены примеры агрессий в сети, введения новых понятий (флеминг, троллинг, хейтинг, кибersталкинг, кибербуллинг). Обучающиеся разбирают поведенческие особенности детей, попавших в Интернет-зависимость. Разработка практико-ориентированных задачи.
Основы интеграции вопросов кибербезопасности в содержание школьных предметов	Значимость включения вопросов кибербезопасности в содержание общего образования. Анализ содержания учебников по информатике с точки зрения возможностей интеграции вопросов кибербезопасности в содержание учебных программ. Демонстрация педагогического опыта подготовки действующих и будущих учителей к преподаванию основ кибербезопасности.

В рамках курса педагоги не только изучат понятие киберпреступления, виды интернет-мошенничества, средства и методы снижения рисков использования сети Интернет, программное обеспечение для защиты от киберпреступлений, поведенческие особенности детей, попавших в Интернет-зависимость, но и определят значимость включения вопросов кибербезопасности в содержание общего образования, проведут анализ содержания учебников по информатике для 5–11 классов с точки зрения возможностей интеграции вопросов кибербезопасности в содержание учебных программ, изучат педагогический опыт подготовки действующих и будущих учителей информатики к преподаванию основ кибербезопасности. Кроме того, педагоги познакомятся

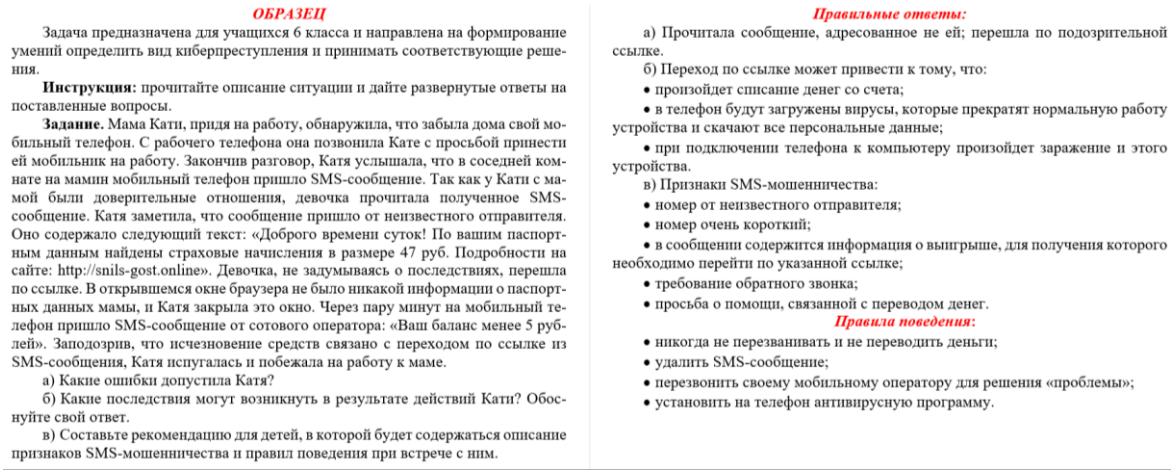
с методическими особенностями обучения учащихся основам кибербезопасности: средства, методы, формы организации учебных занятий.

Методика проведения лекционных и практических занятий предполагает постановку перед слушателями контекстных задач, которые позволят повысить уровень сформированности умений и навыков в области кибербезопасности самих учителей, а также повысить мотивацию в освоении педагогических инструментов формирования у учащихся навыков безопасной работы в киберпространстве.

Пример 1. Представьте, что Вы являетесь руководителем образовательной организации. Вам необходимо определить цифровой след претендента на должность заместителя директора по учебной работе. В качестве исходных данных выступает резюме претендента. Составьте подробный план (не менее 5 пунктов), по которому Вы будете действовать, с указанием ожидаемых результатов поиска информации.

Предполагается, что учителя будут не только выполнять практические задания, но также и разрабатывать их самостоятельно для школьников.

Пример 2. Разработайте проблемные ситуации (не менее 5), которые вовлекают учащихся в деятельность опознавания киберугроз и принятия соответствующих решений (см. образец). Укажите класс и темы в области кибербезопасности, которые раскрываются в данных ситуациях. Представьте решение каждой проблемной ситуации, которое Вы ожидаете от учащихся данного класса.



ОБРАЗЕЦ

Задача предназначена для учащихся 6 класса и направлена на формирование умений определить вид киберпреступления и принимать соответствующие решения.

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.

Рисунок 2 — Образец создания проблемной ситуации

На практических занятиях слушатели разрабатывают сценарии учебных занятий, лекцию «Информационная безопасная среда дома» для родителей, интерактивные игры, веб-квесты, постеры. При этом учителя учитывают тот факт, что у большинства школьников есть опыт работы в киберпространстве и, возможно, они уже сталкивались с киберугрозами. Именно поэтому педагоги разрабатывают методические материалы с опорой на теорию И. С. Якиманской, которая доказала необходимость учета субъектного опыта детей в процессе обучения.

Пример 3. Представьте, что Вы являетесь классным руководителем в 6 классе. Разработайте фрагмент беседы с учащимися, которую Вы проведете с целью обоснования необходимости защиты цифрового следа.

Итоговая аттестация предполагает защиту проектной работы. Слушатели могут выбрать одну из тем: «Внеучебное занятие по кибербезопасности», «Видеоролик “Киберпространство — в чем его опасность?”», «Социальная реклама “Как ты можешь противостоять киберугрозе?”», «Лучший веб-квест по кибербезопасности».

Опыт реализации курса «Обучение основам кибербезопасности в образовательных организациях» осенью 2021 года свидетельствует о том, что педагоги не только смогли повысить уровень сформированности собственных умений и навыков в области кибербезопасности, но и овладели методикой обучения школьников кибербезопасности.

Список литература

1. *Концепция* Стратегии кибербезопасности Российской Федерации. URL: http://council.gov.ru/services/discussions/themes/38324/ (дата обращения: 06.02.2022). Текст: электронный.

2. *Методические* рекомендации «Основы кибербезопасности». Описание курса для средних школ: 2–11 классы / И. М. Тонких [и др.]. Текст: электронный // Вестник образования. 2017. № 18. С. 8–34. URL: http://vestnik.apkpro.ru/doc/osnovi_kiberbezopasnosti.pdf.

3. Парламентские слушанья «Актуальные вопросы обеспечения безопасности и развития детей в информационном пространстве». Текст: электронный // СФ: официальный сайт Совета Федерации Федерального Собрания Российской Федерации. URL: http://council.gov.ru/activity/activities/parliamentary/79549/ (дата обращения: 06.02.2022).

4. *Федеральный* закон «О защите детей от информации, причиняющей вред их здоровью и развитию» от 29.12.2010 № 436-ФЗ. Текст: электронный // КонсультантПлюс. URL: http://www.consultant.ru/document/cons_doc_LAW_108808/ (дата обращения: 06.02.2022).

5. *Федеральный* закон «Об основных гарантиях прав ребенка в Российской Федерации» от 24.07.1998 № 124-ФЗ. Текст: электронный // КонсультантПлюс. URL: http://www.consultant.ru/document/cons_doc_LAW_19558/ (дата обращения: 06.02.2022).