

DOI: 10.32517/2221-1993-2024-23-5-37-42

Е. Д. Иванова, Н. К. Нателаури*Московский педагогический государственный университет, г. Москва, Россия*

НЕКОТОРЫЕ АСПЕКТЫ ОБУЧЕНИЯ ШКОЛЬНИКОВ VII—IX КЛАССОВ БЕЗОПАСНОМУ ПОВЕДЕНИЮ В СОЦИАЛЬНЫХ СЕТЯХ

Аннотация

Статья посвящена основным вопросам безопасного поведения школьников VII—IX классов в социальных сетях. Обосновывается актуальность обучения школьников вопросам безопасного поведения в социальных сетях. Предложено описание курса внеурочной деятельности для учащихся основной школы «Твоя личная безопасность в социальных сетях», направленного на формирование у школьников безопасного поведения в социальной сети. Представлено содержание и приводятся примеры практических заданий, которые учитель может использовать при организации занятий с учащимися, как в урочное, так и во внеурочное время. Раскрываются такие вопросы, как: защита профиля в социальной сети; содержание, размещаемое в сети; медиаграмотность; сетевой этикет и коммуникация; травля и кибербуллинг; мошенничество; защита своих прав и поддержка ментального здоровья. Подробно рассмотрено исследовательское задание «Опасности, которые подстерегают нас в социальных сетях».

Ключевые слова: информатика, безопасное поведение в социальных сетях, основное общее образование.

1. Актуальность обучения школьников VII—IX классов вопросам безопасного поведения в социальных сетях

Обеспечение информационной безопасности, под которой понимается «состояние защищенности информации, которой обладает человек, исключение недопустимых рисков ее уничтожения, искажения и утечки, которые могут привести к невосполнимым потерям или ущербу для лица, обладающего этой информацией» [4], — в настоящее время стало одной из важнейших задач современного общества, отмеченных в ряде указов Президента РФ [12, 13].

Согласно материалам, представленным благотворительным проектом «VK Добро», половина российских школьников имеют аккаунты в социальных сетях [1].

И в этих сетях ребята сталкиваются с такими угрозами и рисками, как нежелательное содержание, опасные знакомства, травля, утечка данных. Вопросы личной безопасности именно в социальных сетях становятся чрезвычайно актуальными для подростков, активно использующих в своей повседневной жизни социальные сети, которые являются для них коммуникационной средой.

Формирование навыков безопасного поведения в Сети, в том числе в социальных сетях, стало неотъемлемой частью образования школьников, нашедшей отражение в ФГОС основного общего образования — в перечне как планируемых личностных, так и метапредметных и предметных результатов по информатике, например [9]:

- 1) личностные результаты: активное неприятие асоциальных поступков, в том числе в сети Интернет;

Контактная информация

Иванова Екатерина Дмитриевна, магистрант кафедры теории и методики обучения математике и информатике, Институт математики и информатики, Московский педагогический государственный университет, г. Москва, Россия; *адрес:* 119991, Россия, г. Москва, ул. Малая Пироговская, д. 1, стр. 1; *e-mail:* katerina2001kat@gmail.com

Нателаури Нино Карловна, канд. пед. наук, доцент, доцент кафедры теории и методики обучения математике и информатике, Институт математики и информатики, Московский педагогический государственный университет, г. Москва, Россия; *адрес:* 119991, Россия, г. Москва, ул. Малая Пироговская, д. 1, стр. 1; *e-mail:* nnatelauri@yandex.ru

E. D. Ivanova, N. K. Natelauri

Moscow Pedagogical State University, Moscow, Russia

SOME ASPECTS OF TEACHING SCHOOLCHILDREN IN GRADES 7–9 SAFE BEHAVIOR IN SOCIAL NETWORKS

Abstract

The article is devoted to the main issues of safe behavior of schoolchildren of grades 7–9 in social networks. The relevance of teaching schoolchildren about safe behavior in social networks is substantiated. The description of the extracurricular activity course for basic school students “Your personal safety in social networks” is proposed, aimed at forming safe behavior in the social network among schoolchildren. The content is presented and examples of practical tasks are given that a teacher can use when organizing classes with students, both during regular and after-school hours. Issues such as: protection of a profile on a social network; content posted on the network; media literacy; network etiquette and communication; bullying and cyberbullying; fraud; protection of one’s rights and mental health support are disclosed. The research task “The dangers that lie in wait for us on social networks” is considered in detail.

Keywords: informatics, safe behavior in social networks, basic general education.

формирование навыков безопасного поведения в интернет-среде;

- 2) метапредметные результаты: выбирать, анализировать, систематизировать и интерпретировать информацию различных видов и форм представления;
- 3) предметные результаты (информатика): умение выбирать безопасные стратегии поведения в сети; умение обеспечивать личную безопасность при использовании ресурсов сети Интернет; умение распознавать попытки и предупреждать вовлечение себя и окружающих в деструктивные и криминальные формы сетевой активности.

В настоящее время интерес с точки зрения формирования навыков безопасного поведения в социальной сети представляют материалы таких авторов, как Л. Л. Босова, А. Ю. Босова, Е. А. Зотова, М. И. Лебешева, Н. Н. Самылкина, Г. У. Солдатов, К. А. Соломина, Г. А. Федорова, И. Ю. Хлобыстова, М. С. Цветкова, В. Н. Шляпников [2, 3, 5, 6, 11, 14, 15] и др., в которых:

- рассматривается определение социальной сети;
- приведены правила сетевого этикета, которых необходимо придерживаться при использовании сервисов интернет-коммуникаций;

- перечислены основные опасности, с которыми может столкнуться пользователь в интернете, в том числе в социальных сетях (контакты с незнакомыми людьми, фишинг, нежелательные для просмотра или использования материалы);
- представлены практические работы, вопросы для самопроверки, кейсы и др.

Анализ имеющихся по теме материалов позволил разработать и подобрать дополнительные задания, которые учитель может использовать как в урочной, так и во внеурочной деятельности школьников в рамках изучения тематического раздела «Цифровая грамотность». С точки зрения внеурочных занятий для формирования навыков безопасного поведения школьников в социальных сетях интерес представляет курс «Твоя личная безопасность в социальных сетях».

2. Курс для учащихся VII—IX классов по безопасному поведению в социальной сети

Курс «Твоя личная безопасность в социальных сетях» рассчитан на 16 часов и включает в себя темы, указанные в таблице.

2.1. Содержание курса «Твоя личная безопасность в социальных сетях»

Таблица

Темы курса внеурочной деятельности «Твоя личная безопасность в социальных сетях»

№ п/п	Тема	Содержание темы
1	Введение в социальные сети. Роль социальных сетей в нашей жизни	Понятие социальных сетей: определение, основные функции. Направления деятельности школьников в сети. История развития социальных сетей. <i>Примеры практических работ:</i> • Найти и подписаться на группу в социальной сети, которая предлагает полезные материалы и задания для подготовки к ОГЭ по информатике или другому предмету. Обратить внимание на качество содержания и активность участников. • В парах выбрать тему, которая заинтересовала бы обоих участников. Найти группы или сообщества в социальных сетях, связанные с выбранной темой. Подписаться на эти группы (сообщества) и изучить предлагаемые материалы. В конце занятия предложить каждой паре представить классу наиболее интересную группу из тех, на которые они подписались.
2	Создание страницы (группы) в социальной сети	Рассматривается понятие ролей в группе, как должны выглядеть план публикаций и материалы, размещаемые на странице группы. <i>Пример проектной работы по теме «Создание группы в социальной сети»:</i> • Выбрать тему проекта (работа в группе). Распределить роли в группе. Обсудить план работы по реализации проекта. (Реализовывать проект, уточнять информацию, выкладываемую в группе, предлагается по мере знакомства с основными темами курса.)
3	Опасности, которые подстерегают нас в социальных сетях	Знакомство с понятиями: пользователь, пространство пользователя, профиль. <i>Пример практической работы:</i> • Анализ профиля Вадима (вымышленного школьника) по заранее подготовленным учителем материалам (описание задания приводится в разделе 2.2).
4	Сильные пароли	Обеспечение своей безопасности в социальных сетях, меры защиты своего аккаунта, своих данных и личной информации. Понятия слабого и сильного пароля, требования к паролям, спецсимволы, криптостойкость, уникальность пароля. Генераторы паролей и их использование при создании своего пароля. <i>Примеры практических работ:</i> • Найти в интернете генераторы паролей. Изучить их основные возможности (например: возможность указания длины пароля, используемых символов, указа-

Продолжение табл.

№ п/п	Тема	Содержание темы
		ния надежности и т. д.). Сгенерировать несколько паролей. Проверить их на надежность с помощью https://password.kaspersky.com/ru/. Сделать выводы о правилах составления надежного пароля. - Предложить распознать слабые и сильные (надежные) пароли среди предложенного учителем перечня. Например: pYhATW (слабый, слишком короткий), левитация (слабый, слишком короткий пароль, засветился в базах утекших паролей), uvvJjXDFbk (слабый, не хватает разнообразия знаков), 8y—@s*gVTRE2t7, (надежный пароль, но сложно запоминаемый), tri3devushki_pod_oknom (надежный пароль) и др. - Придумать свой пароль и проверить его на надежность. - Изменить пароль к своему аккаунту, если этот пароль слабый.
5	Двухфакторная аутентификация. Настройки страницы	Почему важно защищать свою личную информацию в интернете. Понятие двухфакторной аутентификации; необходимость использования данного метода в социальных сетях. Открытые и закрытые профили. Как закрыть профиль в социальных сетях? Как понять, что вас взломали, и что делать? <i>Пример практикума:</i> Проверка надежности аккаунта.
6	Содержание, размещаемое в сети	Содержание, размещаемое пользователем в сети. Разрешенное и запрещенное содержание. Законодательная база. Авторское право. <i>Пример практической работы (кейсы):</i> Предлагаются ситуации, которые отражают нарушения в социальных сетях. Необходимо найти закон, который позволит защитить права пользователя в выданных учителем ситуациях (организация поиска соответствующих законов на информационно-правовых порталах или конкретных статей в выданных учителем материалах). Примеры ситуаций: оскорбление, клевета, распространение в сети персональных данных человека, сведений о частной жизни без его согласия, кражи интеллектуальной собственности и др.
7	Доверяй, но проверяй — урок медиаграмотности	Понятие медиаграмотности, навыки медиаграмотности, достоверная информация, фейковая информация. Какие шаги необходимо предпринять, чтобы проверить достоверность информации. Какие последствия могут быть при распространении недостоверной информации в Сети. <i>Пример практической работы:</i> - Анализ предложенного содержания на поиск ошибок и достоверность. Примеры содержания: «Летающие пингвины» (фильм ВВС); - изображение айсберга на фотографии Р. Клевенджера; - ошибки, допускаемые известными блогерами, и др.
8	Наш цифровой след	Понятие цифрового следа (активный, пассивный), cookies (постоянные, временные). Информация, собираемая социальными сетями. Способы защиты личной информации. <i>Пример практической работы:</i> Анализ своего цифрового следа [10].
9	Коммуникации и этикет в социальной сети	Понятие коммуникации, сетевого этикета. Основные принципы сетевого этикета. Нарушения сетевого этикета. <i>Примеры практических работ:</i> - Изучить изображения элементов диалога или сообщений из социальной сети и выделить нормы, которые были нарушены согласно сетевому этикету (например: изображение диалога, где участник пишет сообщения прописными буквами; избыток эмодзи; массовая рассылка и др.). - Анализ и исправление предложенного диалога (в диалоге используются иностранные и сленговые слова, присутствуют грамматические ошибки в словах). - Организация дебатов. Примерная тема дебатов: «Использование сленга и эмодзи в переписке с друзьями: за и против». Дебаты могут быть реализованы дистанционно, например, с помощью ресурса: https://www.kialo-edu.com/ или его российского аналога.
10	Язык социальных сетей: эмодзи	Понятие эмодзи. Происхождение и история эмодзи. Интерпретация эмодзи. Причины использования. <i>Примеры практических работ:</i> - Отгадайте пословицу, зашифрованную в эмодзи. - Создайте свой уникальный набор эмодзи и стикеров для социальной сети.

Окончание табл.

№ п/п	Тема	Содержание темы
11	Полезные интернет-ресурсы в социальных сетях	Понятия: подкаст, блог, вебинар. Использование подкаста, блога, вебинара в образовательных целях. Этапы разработки подкаста, ведения блога, проведения вебинара. Полезные образовательные интернет-ресурсы в социальной сети. <i>Пример практической работы:</i> Разработка текста подкаста для своей группы в социальной сети. Озвучивание текста с помощью нейросети или запись подкаста. Редактирование аудиозаписи.
12	Кибербуллинг	Понятие травли, буллинга, кибербуллинга. Виды кибербуллинга и его последствия. Что делать, если вы стали жертвой кибербуллинга. Знакомство с законами, защищающими от кибербуллинга. Ресурсы, которые могут помочь, например: https://травлинет.рф/, проект https://kiberbulling.net/ <i>Примеры практических работ:</i> • Определить, является ли приведенная ситуация кибербуллингом, если да, то к какому виду она относится. • Кейс «Продолжай в том же духе!» [5].
13	Мошенничество и фишинг	Особенности мошенничества в социальных сетях. Понятие фишинга и его виды, признаки. История фишинга. Примеры крупных фишинговых атак. <i>Примеры практических работ:</i> • Изучить ресурсы и определить признаки фишинга на них. • Практические работы в формате диалоговых тренажеров [7].
14	Ментальное здоровье в социальной сети	Понятие ментального здоровья. Причины нарушения ментального здоровья. Положительное и негативное влияние социальных сетей на ментальное здоровье человека. Как избежать зависимости от социальных сетей. Баланс между онлайн- и офлайн-жизнью. <i>Пример практической работы:</i> • Оценить количество времени, проведенное в сети Интернет, социальных сетях (заполнить таблицу на основе данных мобильных устройств и сделать выводы).
15	Действия при угрозах в Социальных сетях	Понятия угрозы, тяжкого вреда здоровью. Действия при угрозе. Контакты служб поддержки. Обсуждение того, какой может быть поддержка друга, одноклассника в социальной сети. <i>Примеры практических работ:</i> • Игра «Цепь добра» или ее вариации. Цель игры: научиться оказывать и получать поддержку в социальных сетях, развить эмпатию. Ученику (группе учеников) выдается карточка с заданием: предложить поддерживающее сообщение или комментарий к ситуации, которая может произойти в социальной сети. Обсуждение ситуаций в группе. Учащиеся зачитывают ситуации и предлагаемые поддерживающие сообщения. Примеры ситуаций: – один из ваших одноклассников делится новостью о том, что он принял участие в олимпиаде по искусственному интеллекту, и описывает свои эмоции (например, радость и облегчение от того, что олимпиада закончилась); – кто-то оставляет несправедливые негативные комментарии под фотографией вашего друга в социальной сети и др. • Написать поддерживающее сообщение на странице одноклассника в социальной сети.
16	Тенденции развития социальных сетей. Презентация проектов	Актуальные тенденции в социальных сетях. Понятие короткометражного видео. QR-код в социальных сетях. Аутентичность и искренность в контексте социальных сетей. Визуализация информации с использованием графики, инфографики и визуального контента в социальных сетях. Презентация групповых проектов.

2.2. Задание «Опасности, которые подстерегают нас в социальных сетях»

«Опасности, которые подстерегают нас в социальных сетях» — исследовательское задание с опорой на аккаунт пользователя — сверстника обучающихся. Этот аккаунт создается учителем на основе анализа аккаунтов детей возраста 14–16 лет. Если есть возможность, аккаунт может быть создан в социальной сети, наиболее часто используемой школьниками на момент создания, или

это может быть интерактивный ресурс, внешне схожий с социальной сетью.

Цель задания: обратить внимание обучающихся на контент, выкладываемый в Сеть для общего доступа, и опасности, с которыми ребята могут столкнуться, если не соблюдать правила безопасного поведения в интернет-среде.

Профиль пользователя Вадима (вымышленный). Для создания профиля Вадима учителю необходимо подготовить его словесное описание. Ниже приводится пример подобного описания.



Рис. Вадим (изображение создано с помощью нейросети)

Вадим, 14 лет, учится в седьмом классе общеобразовательной школы. Иногда у него возникают трудности с точными науками, особенно трудно ему в математике. Любит играть в футбол и участвует в школьной команде. У него есть несколько близких друзей, с которыми он проводит много времени после уроков. Вадим общительный и дружелюбный парень, который всегда готов помочь своим товарищам. У него есть домашний питомец — кот по имени Сникерс, которого он очень любит и уделяет ему много внимания. Сникерс ласковый и игривый кот, который стал надежным другом и компаньоном для Вадима. Родители Вадима работают в крупной компании, уделяя сыну недостаточное времени. Вадим много времени проводит в социальных сетях, проверяя уведомления и обновления. На своей странице и на страницах друзей он постоянно сравнивает себя с другими пользователями социальных сетей, особенно с теми, кто кажется ему более успешным или популярным.

Учащимся предлагается зайти на страницу Вадима в социальной сети и описать его профиль, опираясь на подготовленные учителем вопросы. Выполнять задание, связанное с анализом открытого профиля Вадима в социальной сети, целесообразнее в парах, что позволит ребятам обмениваться мнениями, идеями.

Вопросы.

Опишите Вадима:

1. Сколько лет Вадиму?

(В профиле выложена фотография со дня рождения Вадима, на которой Вадим стоит с тортом, где написано «13 лет». Фото было выложено год назад. Ребятам необходимо сделать вывод, что на данный момент Вадиму 14 лет.)

2. В каком году родился Вадим?

3. В каком городе проживает Вадим?

(В профиле выложены фотографии, на которых Вадим регулярно посещает стадион «Солидарность Арена». Поиск по фотографии позволит найти информацию, что стадион расположен в городе Самара. Можно сделать предположение, что Вадим проживает именно в этом городе.)

4. Что вы можете сказать о семье пользователя?

(После просмотра представленной на странице информации учащиеся могут сделать вывод, что се-

мья полная, но, так как родители много работают в крупной компании, времени на сына у них остается не очень много (на страницах Вадима мало совместных фотографий).)

5. Что можете сказать о доходах семьи Вадима?

(После просмотра страницы Вадима по размещенным фотографиям можно сказать, что доход семьи высокий.)

6. Есть ли у Вадима домашние животные?

(По информации, выложенной на странице, учащиеся могут определить, что у Вадима есть кот и его зовут Сникерс. Это может быть важным при подборе пароля к профилю Вадима.)

7. Опишите характер Вадима.

(На основе групп, в которые вступил Вадим, общения на странице, оставленных комментариев, записей школьники могут описать характер пользователя: Вадим — человек настроения, достаточно общительный, легко находит общий язык с другими. Он любит получать похвалу и признание своих достижений, что мотивирует его к новым свершениям. В свободное время Вадим предпочитает играть в футбол, посещать интересные места в городе и планировать будущие путешествия. Вместе с тем, исходя из представленного описания характера Вадима, его склонностей к получению похвалы, зависимости от мнения окружающих, его эмоциональности и стремления к идеализации себя в виртуальном мире, ребята могут сделать вывод, что Вадим может быть уязвим перед внешним влиянием, особенно, если это влияние маскируется под поддержку или одобрение [8].)

8. Можно ли взломать пароль Вадима? Предложить школьникам подобрать пароль.

(Можно предположить, что его пароль — из списка наиболее часто используемых паролей или состоит из его имени и года рождения, или клички домашнего животного и года его рождения и т. д.)

9. Почему вы смогли увидеть все данные, выложенные Вадимом в своем профиле?

(Потому что это открытый профиль, вся информация видна.)

В конце занятия предлагается коллективно обсудить получившиеся ответы на поставленные вопросы. Одним из основных вопросов, который стоит обсудить с ребятами: **«Каким образом злоумышленник может навредить Вадиму, выяснив о нем ту информацию, которую смогли выяснить вы?»**

Другие вопросы для обсуждения:

- Много ли информации о профиле Вадима мы узнали? (Да.)
- Почему? (У Вадима много личных данных в социальных сетях.)
- Какими личными данными вы обычно делитесь в социальных сетях?
- А мог ли Вадим обезопасить себя и не дать посторонним людям ознакомиться с его личной информацией? (Мог, создав закрытый аккаунт.)
- Будет ли «аккаунт в безопасности», если закрыть его?
- Сталкивались ли вы или ваши знакомые со взломом их страниц в социальной сети?

Итогом такой игры может стать вывод о том, что любой человек, который заходит на страницу пользователя социальной сети, может узнать о нем много информации, если пользователь не будет задумываться о своей безопасности. Учащиеся увидят, что распространение информации, фотографий и т. д. в своих социальных сетях или в социальных сетях родителей может привлечь внимание злоумышленников и одна из первых мер обезопасить свой профиль — сделать его закрытым.

3. Заключение

В современном обществе каждого гражданина сопровождают возрастающие вызовы, связанные с безопасностью в интернете, особенно в контексте использования социальных сетей. С увеличением объемов и значимости данных, передаваемых и обрабатываемых в сети, вопрос личной безопасности становится чрезвычайно актуальным для всех. К сожалению, несмотря на включение указанных выше вопросов в курс информатики основной школы, ограниченность в урочных часах на базовом уровне не дает возможности еще на ранних этапах познакомить школьников с безопасным поведением в социальной сети и выработать у них безопасную стратегию поведения. В связи с этим, надеемся, предлагаемые вопросы, затронутые в статье, будут интересны учителям информатики.

Список источников

1. 70 % родителей — в друзьях с детьми в соцсетях // VK Добро. <https://dobro.mail.ru/stories/ya-u-tebya-v-druzyah-istavlyu-lajki/>
2. Босова Л. Л., Босова А. Ю. Информатика. 7 класс: учебник. 3-е изд., стер. М.: БИНОМ. Лаборатория знаний, 2021. 239 с. EDN: NNRIFB.
3. Босова Л. Л., Босова А. Ю. Информатика. 9 класс: учебник. 3-е изд., стер. М.: Просвещение, 2022. 208 с. EDN: OOJGYD.
4. Босова Л. Л., Босова А. Ю. Об информационной безопасности в общеобразовательной школе // Актуальные вопросы методики обучения информатике в условиях цифровой трансформации образования. М.: МПГУ, 2024. С. 91–102. EDN: PAXWXA.
5. Босова Л. Л., Самылкина Н. Н. Система оценки достижений планируемых предметных результатов освоения учебного предмета «Информатика»: методические рекомендации. М.: ФГБНУ «Институт стратегии развития образования РАО», 2023. 83 с. EDN: UOIWQH.
6. Босова Л. Л., Самылкина Н. Н. Формирование цифровых компетенций в области информационной этики и права в курсе школьной информатики // Актуальные вопросы методики обучения информатике в условиях цифровой трансформации образования. М.: Московский педагогический государственный университет, 2024. С. 103–111. EDN: GKKKZC.
7. Дорохова А. А. Формирование цифровых компетенций в области информационной этики и права с помощью кейсов по социальной инженерии // Актуальные проблемы методики обучения информатике и математике в современной школе. Материалы международной научно-практической интернет-конференции (Москва, 18–24 апреля 2022 года). М.: МПГУ, 2022. С. 108–115. EDN: JVOBQH.
8. Зиновьева А. Р. Вовлеченность молодежи в деструктивные группы сети Интернет как психологическая проблема // Прикладная психология и психоанализ: электронный научный журнал. 2020. № 1. EDN: TKXXSQ. <https://clck.ru/3Dai22>
9. Приказ Министерства просвещения Российской Федерации от 31 мая 2021 г. № 287 «Об утверждении федерального государственного образовательного стандарта основного общего образования». https://edsoo.ru/wp-content/uploads/2023/08/Приказ-№-287-от-31.05.2021-ФГОС_ООО.pdf
10. Салахова А. А. Искусственный интеллект в образовании: что такое цифровой след и как его анализировать // Актуальные проблемы методики обучения информатике и математике в современной школе. Материалы международной научно-практической интернет-конференции (Москва, 18–24 апреля 2022 года). М.: МПГУ, 2022. С. 320–324. EDN: GTZUXE.
11. Солдатова Г. У., Зотова Е. А., Лебешева М. И., Шляпников В. Н. Интернет: возможности, компетенции, безопасность: методическое пособие для работников системы общего образования. М.: Центр книжной культуры «Гутенберг», 2013. 165 с. EDN: ZTWDZF.
12. Указ Президента Российской Федерации от 05.12.2016 г. № 646 «Об утверждении Доктрины информационной безопасности Российской Федерации». <http://www.kremlin.ru/acts/bank/41460/page/1>
13. Указ Президента Российской Федерации от 09.05.2017 г. № 203 «О Стратегии развития информационного общества в Российской Федерации на 2017–2030 годы». <http://www.kremlin.ru/acts/bank/41919/page/1>
14. Федорова Г. А., Соломина К. А. Дистанционная олимпиада для учащихся VII–IX классов «Этические и правовые основы взаимодействия в социальных сетях» // Информатика в школе. 2022. № 5. С. 32–38. EDN: GTPRTK. DOI: 10.32517/2221-1993-2022-21-5-32-38.
15. Цветкова М. С., Хлобыстова И. Ю. Информационная безопасность. Кибербезопасность. 7–9 классы: учебное пособие. 2-е изд., пересм. М.: БИНОМ. Лаборатория знаний, 2020. 64 с. EDN: UFPSGW.