

**Государственное бюджетное общеобразовательное учреждение
Самарской области средняя общеобразовательная школа
с. Верхние Белозерки муниципального района Ставропольский
Самарской области.**

РАССМОТРЕНО
Руководитель МО
Мурыгина К.А.

Протокол
№1 от _27.08.2024_

СОГЛАСОВАНО
Заместитель директора по
УВР
Горбункова С.А

Протокол пед.совета №1
От 27.08.2024

УТВЕРЖДЕНО
Директор
Полякова В.В

Приказ № _56-од
от 27.08.2024

Программа внеурочной деятельности

«Информационная безопасность»

7 класс

Разработала: Кромская И.А.

2024г.

Пояснительная записка

Программа курса «Цифровая гигиена»¹ адресована учащимся 7-9 классов, а также их родителями учитываются требования, выдвигаемые федеральным государственным образовательным стандартом основного общего образования к предметным (образовательные области «Математика и информатика», «Физическая культура, экология и ОБЖ»), метапредметным и личностным результатам.

Основными целями изучения курса «Цифровая гигиена» являются:

- обеспечение условий для профилактики негативных тенденций в информационной культуре учащихся, повышения защищенности детей от информационных рисков и угроз;
- формирование навыков своевременного распознавания онлайн-рисков (технического, контентного, коммуникационного, потребительского характера и риска интернет-зависимости).

Задачи программы:

- сформировать общекультурные навыки работы с информацией (умения, связанные с поиском, пониманием, организацией, архивированием цифровой информации и ее критическим осмыслением, а также созданием информационных объектов с использованием цифровых ресурсов (текстовых, изобразительных, аудио и видео);
- создать условия для формирования умений, необходимых для различных форм коммуникации (электронная почта, чаты, блоги, форумы, социальные сети и др.) с различными целями и ответственными отношениями к взаимодействию в современной информационно-телекоммуникационной среде;
- сформировать знания, позволяющие эффективно и безопасно использовать технические и программные средства для решения различных задач, в том числе использования компьютерных сетей, облачных сервисов и т.п.;
- сформировать знания, умения, мотивацию и ответственность, позволяющие решать с помощью цифровых устройств и интернета различные повседневные задачи, связанные с конкретными жизненными ситуациями, предполагающими удовлетворение различных потребностей;
- сформировать навыки по профилактике и коррекции зависимого поведения школьников, связанного с компьютерными технологиями и Интернетом.

Общая характеристика учебного курса

¹Программа курса «Цифровая гигиена» разработана на основе программы курса «Информационная безопасность, или Нарастающий риск одного вируса» Наместниковой М.С.

Курс «Цифровая гигиена» является важной составляющей работы с обучающимися, активно использующими различные сетевые формы общения (социальные сети, игры, пр.) с целью мотивации ответственного отношения к обеспечению своей личной безопасности, безопасности своей семьи и своих друзей. Кроме того, реализация курса создаст условия для сокращения цифрового разрыва между поколениями и позволит родителям выступать в качестве экспертов, передающих опыт.

Данный курс предполагает организацию работ в соответствии с содержанием 2-х модулей, предназначенных для обучающихся 7 класса и родителей обучающихся любого возраста соответственно.

Модуль 1.

Отбор тематики содержания курса осуществлен с учетом целей и задач ФГОС основного общего образования, возрастных особенностей и познавательных возможностей обучающихся 7 класса.

В преподавании курса «Цифровая гигиена» могут использоваться разнообразные форматы обучения: традиционный урок (коллективная и групповая формы работы), тренинги (в классической форме или по кейс-методу), дистанционное обучение (электронные курсы, видеоролики, почтовые рассылки, микрообучение), смешанный формат.

Система учебных заданий должна создавать условия для формирования активной позиции школьников в получении знаний и умений выявлять информационную угрозу, определять степень ее опасности, предвидеть последствия информационной угрозы и противостоять им и профилактике негативных тенденций в развитии информационной культуры учащихся, повышения защищенности детей от информационных рисков и угроз (составление памяток, анализ защищенности собственных аккаунтов в социальных сетях и электронных сервисах, практически работы и т.д.).

Место учебного курса (Модуль 1) в учебном плане

Программа учебного курса (Модуль 1) рассчитана на 34 учебных часа, из них 22 часа – учебных занятий, 9 часов – подготовка и защита учебных проектов, 3 часа – повторение. На изучение модуля 1 курса «Цифровая гигиена» отводится по 1 часу в неделю в 7 классе, Учебные занятия по программе могут быть реализованы в различных вариантах:

- 1) в течение одного учебного года в 7 классе. В этом случае программа рассчитана на 34 учебные недели;
- 2) по одному разделу последовательно в 7 классе;
- 3) произвольно распределены учителям в зависимости от интереса и готовности школьников.

Характеристика личностных, метапредметных и предметных результатов освоения учебного курса (Модуль 1)²

Предметные:

Выпускник научится:

- анализировать доменные имена компьютеров и адреса документов в интернете;
- безопасно использовать средства коммуникации,
- безопасно вести и применять способы самозащиты при попытке мошенничества,
- безопасно использовать ресурсы интернета.

Выпускник овладеет:

- приемами безопасной организации своего личного пространства данных с использованием индивидуальных накопителей данных, интернет-сервисов и т.п.

Выпускник получит возможность овладеть:

- основами соблюдения норм информационной этики и права;
- основами самоконтроля, самооценки, принятия решений и осуществления осознанного выбора в учебной и познавательной деятельности при формировании и современной культуры безопасности жизнедеятельности;
- использовать для решения коммуникативных задач в области безопасности жизнедеятельности различные источники информации, включая Интернет-ресурсы и другие базы данных.

Метапредметные.

Регулятивные универсальные учебные действия.

В результате освоения учебного курса обучающийся сможет:

- идентифицировать собственные проблемы и определять главную проблему;
- выдвигать версии решения проблемы, формулировать гипотезы, предвосхищать конечный результат;
- ставить цель деятельности на основе определенной проблемы и существующих возможностей;
- выбирать из предложенных вариантов самостоятельно искать средства/ресурсы для решения задачи/достижения цели;
- составлять план решения проблемы (выполнения проекта, проведения исследования);
- описывать свой опыт, оформляя его для передачи другим людям

²Примерная основная образовательная программа основного общего образования // http://fgosreestr.ru/registry/pri_mernaya-osnovnaya-obrazovatel'naya-programma-osnovnogo-obshhego-obrazovaniya-3/

видетехнологиирешенияпрактическихзадачопределенногокласса;

- оцениватьсвоюдеятельность,аргументируяпричиныдостиженияилиотсутствияпланируемогорезультата;
- находить достаточные средства для выполнения учебных действий вменяющейсяситуацииилиприотсутствиипланируемогорезультата;
- работаяпосвоемуплану,вноситькоррективывтекущуюдеятельностьнаосновеанализаизмененийситуациидляполучениязапланированныххарактеристикпродукта/результата;
- приниматьрешениевучебнойситуацииинестиэтогоответственность.

Познавательныеуниверсальныеучебныедействия.

Врезультатеосвоенияучебногокурсаобучающийсяможет:

- выделятьявлениеизобщегорядадругихявлений;
- определять обстоятельства, которые предшествовали возникновениюсвязимеждуявлениями,изэтихобстоятельстввыделятьопределяющие,способныебытьпричинойданногоявления,выявлятьпричиныиследствияявлений;
- строитьрассуждениеотобщихзакономерностейкчастнымявлениямиотчастныхявленийкобщимзакономерностям;
- излагатьполученнуюинформацию,интерпретируяеевконтекстерешаемойзадачи;
- самостоятельноуказыватьнаинформацию,нуждающуюсявпроверке,предлагатьиприменятьспособпроверкидостоверностиинформации;
- критическиоцениватьсодержаниеиформутекста;
- определятьнеобходимыеключевыепоисковыесловаизапросы.

Коммуникативныеуниверсальныеучебныедействия.

Врезультатеосвоенияучебногокурсаобучающийсяможет:

- строитьпозитивныеотношениявпроцессеучебнойипознавательнойдеятельности;
- критическиотноситьсяксобственномумнению,сдостоинствомпризнаватьошибочностьсвоегомнения(еслионотакое)икорректироватьего;
- договариватьсяоправилахивопросахдляобсуждениявсоответствииисоставленнойпередгруппойзадачей;
- делатьоценочныйвывододостижениицеликоммуникациинепосредственнопослезавершениякоммуникативногоконтактаиобосновыватьего.
- целенаправленноискатьииспользоватьинформационныересурсы,необходимыедлярешенияучебныхипрактическихзадачспомощьюсредствИКТ;

- выбирать, строить и использовать адекватную информационную модель для передачи своих мыслей средствами естественных и формальных языков в соответствии с условиями коммуникации;
- использовать компьютерные технологии (включая выбор адекватных задаче инструментальных программно-аппаратных средств и сервисов) для решения информационных и коммуникационных учебных задач, в том числе: вычисление, написание писем, сочинений, докладов, рефератов, создание презентаций и др.;
- использовать информацию с учетом этических и правовых норм;
- создавать информационные ресурсы разного типа и для разных аудиторий, соблюдать информационную гигиену и правила информационной безопасности.

Личностные.

- осознанное, уважительное и доброжелательное отношение к окружающим людям в реальном и виртуальном мире, их позициям, взглядам, готовность вести диалог с другими людьми, обоснованно осуществлять выбор виртуальных собеседников;
- готовность и способность к осознанному выбору и построению дальнейшей индивидуальной траектории образования на базе ориентировки в мире профессий и профессиональных предпочтений, с учетом устойчивых познавательных интересов;
- освоенность социальных норм, правил поведения, ролей и форм социальной жизни в группах и сообществах;
- сформированность ценности безопасного образа жизни; интериоризация правил индивидуального и коллективного безопасного поведения в информационно-телекоммуникационной среде.

Содержание программы учебного курса (Модуль 1).

Содержание программы учебного курса (Модуль 1) соответствует темам примерной основной образовательной программы основного общего образования (ООПОО) по учебным предметам «Информатика» и «Основы безопасности жизнедеятельности», а также расширяет их за счет привлечения жизненного опыта обучающихся в использовании всевозможных технических устройств (персональных компьютеров, планшетов, смартфонов и пр.), позволяет правильно вести ребенка в цифровое пространство и корректировать его поведение в виртуальном мире.

Основное содержание программы представлено разделами «Безопасность общения», «Безопасность устройств», «Безопасность информации».

Каждый раздел учебного курса (Модуля 1) завершается выполнением проектной работы по одной из тем, предложенных на выбор учащихся и/или проверочного теста.

За счет часов, предусмотренных для повторения материала (4 часа), возможно проведение занятий для учащихся 4-б классов. Эти занятия в качестве волонтерской практики могут быть проведены учащимися, освоившими программу. Для проведения занятий могут быть использованы презентации, проекты, памятки, онлайн-занятия, подготовленные в ходе выполнения учебных заданий по основным темам курса.

Содержание учебного курса (Модуль 1).

Раздел 1. «Безопасность общения»

Тема 1. Общение в социальных сетях и мессенджерах. 1 час.

Социальная сеть. История социальных сетей. Мессенджеры. Назначение социальных сетей и мессенджеров. Пользовательский контент.

Тема 2. С кем безопасно общаться в интернете. 1 час.

Персональные данные как основной капитал личного пространства в цифровом мире. Правила добавления друзей в социальных сетях. Профиль пользователя. Анонимные социальные сети.

Тема 3. Пароли для аккаунтов социальных сетей. 1 час.

Сложные пароли. Онлайн-генераторы паролей. Правила хранения паролей. Использование функции браузера по запоминанию паролей.

Тема 4. Безопасный вход в аккаунты. 1 час.

Виды аутентификации. Настройки безопасности аккаунта. Работа на чужом компьютере: точки зрения безопасности личного аккаунта.

Тема 5. Настройки конфиденциальности в социальных сетях. 1 час.

Настройки приватности и конфиденциальности в разных социальных сетях. Приватность и конфиденциальность в мессенджерах.

Тема 6. Публикация информации в социальных сетях. 1 час.

Персональные данные. Публикация личной информации.

Тема 7. Кибербуллинг. 1 час.

Определение кибербуллинга. Возможные причины кибербуллинга и как его избежать? Как не стать жертвой кибербуллинга. Как помочь жертве кибербуллинга.

Тема 8. Публичные аккаунты. 1 час.

Настройки приватности публичных страниц. Правила ведения публичных страниц. Овершеринг.

Тема 9. Фишинг. 2 часа.

Фишинг как мошеннический прием. Популярные варианты распространения фишинга. Отличие настоящих и фишинговых сайтов. Как защититься от фишеров в социальных сетях и мессенджерах.

**Выполнение и защита индивидуальных и групповых проектов³.
3 часа.**

Раздел 2. «Безопасность устройств».

Тема 1. Что такое вредоносный код. 1 час.

Виды вредоносных кодов. Возможности и деструктивные функции вредоносных кодов.

Тема 2. Распространение вредоносного кода. 1 час.

Способы доставки вредоносных кодов. Исполняемые файлы и расширения вредоносных кодов. Вредоносная рассылка. Вредоносные скрипты. Способы выявления наличия вредоносных кодов на устройствах. Действия при обнаружении вредоносных кодов на устройствах.

Тема 3. Методы защиты от вредоносных программ. 2 часа.

Способы защиты устройств от вредоносного кода. Антивирусные программы и их характеристики. Правила защиты от вредоносных кодов.

**Тема 4. Распространение вредоносного кода для мобильных устройств.
1 час.**

Расширение вредоносных кодов для мобильных устройств. Правила безопасности при установке приложений на мобильные устройства.

**Выполнение и защита индивидуальных и групповых проектов.
3 часа.**

Раздел 3 «Безопасность информации»

Тема 1. Социальная инженерия: распознать и избежать. 1 час.

Приемы социальной инженерии. Правила безопасности при виртуальных контактах.

Тема 2. Ложная информация в Интернете. 1 час.

³Требования к содержанию итоговых проектно-исследовательских работ содержатся в приложении 1 к данной рабочей программе

Цифровое пространство как площадка самопрезентации, экспериментирования и освоения различных социальных ролей. Фейковые новости. Поддельные страницы.

Тема 3. Безопасность при использовании платежных карт в Интернете. 1 час.

Транзакции и связанные с ними риски. Правила совершения онлайн покупок. Безопасность банковских сервисов.

Тема 4. Беспроводная технология связи. 1 час.

Уязвимость Wi-Fi-соединений. Публичные и непубличные сети. Правила работы в публичных сетях.

Тема 5. Резервное копирование данных. 1 час.

Безопасность личной информации. Создание резервных копий на различных устройствах.

Тема 6. Основы государственной политики в области формирования культуры информационной безопасности. 2 часа.

Доктрина национальной информационной безопасности. Обеспечение свободы и равенства доступа к информации и знаниям. Основные направления государственной политики в области формирования культуры информационной безопасности.

Выполнение и защита индивидуальных и групповых проектов. 3 часа.

Повторение. Волонтерская практика. 3 часа.

Тематическое планирование учебного курса (Модуль 1).

№ п/п	Тема	Количество часов	Основное содержание	Характеристика основных видов учебной деятельности обучающихся
Тема 1. «Безопасность общения»				
1	Общение в социальных сетях и мессенджерах	1	Социальная сеть. История социальных сетей. Мессенджеры. Назначение социальных сетей и мессенджеров. Пользовательский контент.	Выполняет базовые операции при использовании мессенджеров в социальных сетях. Создает свой образ в сети Интернет. Изучает историю и социальную значимость личных аккаунтов в сети Интернет.
2	С кем безопасно общаться в интернете	1	Персональные данные как основная капитал личного пространства в цифровом мире. Правила добавления друзей в социальных сетях. Профиль пользователя. Анонимные социальные сети.	Руководствуется в общении социальными ценностями и установками коллектива и общества в целом. Изучает правила сетевого общения.

3	Пароли для аккаунтов социальных сетей	1	Сложные пароли. Онлайн генератор паролей. Правила хранения паролей. Использование функций браузера по запоминанию паролей.	Изучает основные понятия регистрации информации и шифрования. Умеет их применять
---	---------------------------------------	---	--	--

4	Безопасный вход ваккаунты	1	Виды аутентификации. Настройки безопасности акк аунта. Работа на чужом компьютер есточки зрения безопасности личн ого аккаунта.	Объясняет причины использования безопасного входа при работе на чужом устройстве. Д емонстрирует устойчивый навык б езопасного входа.
5	Настройки конфиденциальности в социальных сетях	1	Настройки приватности и конфиде нциальности в разных социальных сетях. Приватность и конфиденциальность в мессенджерах.	Раскрывает причины установки крытого профиля. Меняет основн ые настройки приватности в личном профиле.
6	Публикация информации в социальны х сетях	1	Персональные данные. Публикация личной информации.	Осуществляет поиск и использует информацию, необходимую для выполнения поставленных задач
7	Кибербуллинг	1	Определение кибербуллинга. Воз можные причины кибербуллинга и как его избежать? Как не стать жертвой кибербуллинга. Как помочь жертв е кибербуллинга.	Реагирует на опасные ситуации, распознает провокации и попытку манипуляции с сторон ы виртуальных собеседников

8	Публичныеаккаунты	1	<p>Настройки приватности публичныхстраниц.Правилаведе нияпубличныхстраниц.Овершер инг.</p>	<p>Решаетэкспериментальныезадач и. Самостоятельно создает источники информации разнотипаидляразныхаудитор ий,</p>
---	-------------------	---	--	---

				соблюдая правила информационной безопасности
9	Фишинг	2	Фишинг как мошеннический прием. Популярны варианты распространения фишинга. Отличие настоящих и фишинговых сайтов. Как защититься от фишеров в социальных сетях и мессенджерах.	Анализ проблемных ситуаций. Разработка кейсов с примерами из личной жизни/жизни знакомых. Разработка распространения чек-листа (памятки) по противодействию фишингу
	Выполнение и защита индивидуальных и групповых проектов	3		Самостоятельная работа
Тема 2. «Безопасность устройств»				
1	Что такое вредоносный код	1	Виды вредоносных кодов. Возможности деструктивные функции вредоносных кодов.	Соблюдает технику безопасности при эксплуатации компьютерных систем. Использует инструментальные программные средства и сервисы адекватно задаче.

2	Распространение вредоносного кода	1	Способы доставки вредоносных кодов. Исполняемые файлы расширения вредоносных кодов. Вредоносная рассылка. Вредоносные скрипты. Способы выявления наличия вредоносных	Выявляет и анализирует (при помощи почечек-листа) возможные угрозы информационной безопасности объектов
---	-----------------------------------	---	--	---

			кодов на устройствах. Действия при обнаружении вредоносных кодов на устройствах.	
3	Методы защиты от вредоносных программ	2	Способы защиты устройств от вредоносного кода. Антивирусные программы их характеристики. Правила защиты от вредоносных кодов.	Изучает виды антивирусных программ и правила их установки
4	Распространение вредоносного кода для мобильных устройств	1	Расширение вредоносных кодов для мобильных устройств. Правила безопасности при установке приложений на мобильные устройства.	Разрабатывает презентацию, инструкцию по обнаружению, алгоритм установки приложений на мобильные устройства для учащихся более младшего возраста.
	Выполнение и защита индивидуальных и групповых проектов	3		Умеет работать индивидуально и в группе. Принимает позицию собеседника, понимая позицию другого, различает в его речи: мнение (точку зрения), доказательство (аргументы), факты; гипотезы, аксиомы, теории
Тема 3 «Безопасность информации»				
1	Социальная инженерия: распознать и избежать	1	Приемы социальной инженерии. Правила безопасности при виртуальных контактах.	Находит нужную информацию в базах данных, составляя запросы на поиск. Систематизирует

				получаемую информацию в процессе поиска.
2	Ложная информация в Интернете	1	Цифровое пространство как площадка для самопрезентации, экспериментирования и освоения различных социальных ролей. Фейковые новости. Поддельные страницы.	Определяет возможные источники необходимых сведений, осуществляет поиск информации. Отбирает и сравнивает материал по нескольким источникам. Анализирует и оценивает достоверность информации.
3	Безопасность при использовании платежных карт в Интернете	1	Транзакции и связанные с ними риски. Правила совершения онлайн покупок. Безопасность банковских сервисов.	Приводит примеры рисков, связанных с совершением онлайн покупок (умеет определить источник риска). Разрабатывает возможные варианты решения ситуаций, связанных с рисками использования платежных карт в Интернете.
4	Беспроводная технология связи	1	Уязвимость Wi-Fi-соединений. Публичные и непубличные сети. Правила работы в публичных сетях.	Используя различную информацию, определяет понятия. Изучает особенности и стиль ведения личных и публичных аккаунтов.

5	Резервное копирование данных	1	Безопасность информации.	личной Создание	Создает резервные копии.
---	------------------------------	---	--------------------------	--------------------	--------------------------

			резервных копий на различных устройствах.	
6	Основы государственной политики в области формирования культуры информационной безопасности	2	<p>Доктрина национальной информационной безопасности. Обеспечение свободы и равенства доступа к информации и знаниям.</p> <p>Основы направления государственной политики в области формирования культуры информационной безопасности.</p>	<p>Умеет привести выдержки из законодательства РФ:</p> <ul style="list-style-type: none"> - обеспечивающего конституционно-правовой поиск, получение и распространение информации; - отражающего правовые аспекты защиты киберпространства.
	Выполнение и защита индивидуальных и групповых проектов	3		
	Повторение, волонтерская практика, резерв	3		
	Итого	34		

Требования к содержанию итоговых проектно-исследовательских работ

Критерии содержания текста проектно-исследовательской работы

1. Вовведение сформулирована актуальность (личностная и социальная значимость) выбранной проблемы. Тема может быть переформулирована, но при этом четко определена, вне необходимости исследования есть аргументы.
2. Правильно составлен научный аппарат работы: точность формулировки проблемы, четкость и конкретность в постановке цели и задач, определении объекта и предмета исследования, выдвижении гипотезы. Гипотеза сформулирована корректно и соответствуют теме работы
3. Есть планирование проектно-исследовательской деятельности, корректировка ее в зависимости от результатов, получаемых на разных этапах развития проекта. Дана характеристика каждого этапа реализации проекта, сформулированы задачи, которые решаются на каждом этапе, в случае коллективного проекта – распределены и выполнены задачи каждым участником, анализ ресурсного обеспечения проекта проведен корректно
4. Используется и осмысливается междисциплинарный подход к исследованию и проектированию и на базовом уровне школьной программы, и на уровне освоения дополнительных библиографических источников
5. Определён объём собственных данных и составлено собственное проектное решение с аналоговыми по проблеме. Дан анализ источников и аналогов в точках зрения значимости для собственной проектно-исследовательской работы, выявлена его новизна, библиография и интернет-ресурсы грамотно оформлены
6. Соблюдены нормы научного стиля изложения и оформления работы. Текст работы должен демонстрировать уровень владения научным стилем изложения.
7. Есть оценка результативности проекта, соотнесение поставленными задачами. Проведена оценка социокультурных и образовательных последствий проекта на индивидуальном и общественном уровнях.

Критерии презентации проектно-исследовательской работы (устного выступления)

1. Демонстрация коммуникативных навыков при защите работы. Владение риторическими умениями, раскрытие автором содержания работы, достаточная осведомленность в терминологической системе проблемы, отсутствие или стических и речевых ошибок, соблюдение регламента.
2. Умение четко отвечать на вопросы после презентации работы.
3. Умение создать качественную презентацию. Демонстрация умения использовать ИТ-технологии и создавать слайд-презентацию соответствующего возрасту уровне.
4. Умение оформлять качественный презентационный буклет соответствующе

мого возрасту уровне.

5. Творческий

подход к созданию продукта, оригинальность, наглядность, иллюстративность.

Предоставлен качественный творческий продукт (макет, программный продукт, стенд, статья, наглядное пособие, литературное произведение, видео-ролик, мультфильм и т.д.).

6. Умение установить отношения коллаборации с участниками проекта, наметить пути создания сетевого продукта. Способность намечать пути сотрудничества на уровне взаимодействия с членами кружка или секции, проявление в ходе презентации и коммуникабельности, благодарности и уважения по отношению к руководителю, консультантам, умение четко обозначить пути создания сетевого продукта.

7. Ярко выраженный интерес к научному поиску, самостоятельность в выборе проблемы, пути ее исследования и проектного решения.

Список источников:

1. Бабаш, А.В. Информационная безопасность: Лабораторный практикум / А.В. Бабаш, Е.К. Баранова, Ю.Н. Мельников. – М.: КноРус, 2019. – 432 с.
2. Вехов В. Б. Компьютерные преступления: способы совершения и раскрытия / В.Б. Вехов; Под ред. акад. Б.П. Смагоринского. – М.: Право и закон, 2014. – 182 с.
3. Громов, Ю.Ю. Информационная безопасность и защита информации: Учебное пособие / Ю.Ю. Громов, В.О. Драчев, О.Г. Иванова. – Ст.Оскол: ТНТ, 2017. – 384 с.
4. Дети в информационном обществе // <http://detionline.com/journal/about>
5. Ефимова, Л.Л. Информационная безопасность детей. Российский и зарубежный опыт: Монография / Л.Л. Ефимова, С.А. Кочерга. – М.: ЮНИТИ-ДАНА, 2016. – 239 с.
6. Запечников, С.В. Информационная безопасность открытых систем. В 2-х т. Т.2 – Средства защиты в сетях / С.В. Запечников, Н.Г. Милославская, А.И. Толстой, Д.В. Ушаков. – М.: ГЛТ, 2018. – 558 с.
7. Защита детей by Kaspersky // <https://kids.kaspersky.ru/>
8. Кузнецова, А.В. Искусственный интеллект и информационная безопасность общества / А.В. Кузнецова, С.И. Самыгин, М.В. Радионов. – М.: Русайнс, 2017. – 64 с.
9. Наместникова М.С. Информационная безопасность, или Нарастающий угроза. 7-9 классы. Внеурочная деятельность. – М.: Просвещение, 2019. – 80 с.
10. Основы кибербезопасности // <https://www.xn--d1abkefqip0a2f.xn--p1ai/index.php/glava-1-osnovy-kiberbezopasnosti-tseli-i-zadachi-kursa>
11. Стрельцов А.А. Правовое обеспечение информационной безопасности России: теоретические и методологические основы. – Минск, 2005. – 304 с.
12. Сусоров И.А. Перспективные технологии обеспечения кибербезопасности // Студенческий: электрон. научн. журн. 2019. №22(66)
13. Цифровая компетентность подростков и родителей. Результаты всероссийского исследования / Г.У. Солдатова, Т.А. Нестик, Е.И. Рассказова, Е.Ю. Зотова. – М.: Фонд Развития Интернет, 2013. – 144 с.