

I. Пояснительная записка.

В основу рабочей программы взяты следующие нормативно-правовые документы:

1. Письмо Минобрнауки России от 12.05.2011 № 03-296 «Об организации внеурочной деятельности при введении федерального государственного образовательного стандарта общего образования»;
2. Закон РФ «Об образовании» (п.16, ст.50)
(«Обучающиеся воспитанники гражданских образовательных учреждений имеют право на свободное посещение мероприятий, не предусмотренных учебным планом»);
3. Национальная образовательная инициатива «Наша новая школа»;
4. Концепция духовно-нравственного развития и воспитания личности гражданина России;
5. Приказ Минобрнауки России от 17 декабря 2010 г. № 1897 «Об утверждении федерального государственного образовательного стандарта основного общего образования»;
6. Письмо Минобрнауки России от 19.04.2011 № 03-255 «О введении федеральных государственных образовательных стандартов общего образования»;
7. Письмо Министерства образования и науки РФ от 12 мая 2011 г. № 03-296 «Об организации внеурочной деятельности при введении федерального государственного образовательного стандарта общего образования»;
8. Письмо Минобрнауки России от 13 мая 2013 года № ИР-352/09 «О направлении программы развития воспитательной компоненты в общеобразовательных учреждениях»;
9. Письмо Минобрнауки России от 12 июля 2013 года № 09-879 «О направлении рекомендаций по формированию перечня мер и мероприятий по реализации Программы развития воспитательной компоненты в общеобразовательной школе»;
10. Положение о внеурочной деятельности ГБОУ СОШ №7 города Похвистнево;
11. Письмо министерства образования и науки Российской Федерации от 14 декабря 2015 № 09-3564 «О внеурочной деятельности и реализации дополнительных общеобразовательных программ»;
12. Письмо министерства образования и науки Самарской области от 17.02.2016 № МО-16-09-01/173-ТУ «О внеурочной деятельности».
13. СанПиН 2.4.2.2821-10 «Санитарно-эпидемиологические требования к условиям и организации обучения в общеобразовательных учреждениях» («Внеурочную деятельность реализуют в виде экскурсий, кружков, секций, олимпиад, соревнований и т.п.»)
14. Примерная рабочая программа учебного курса «Цифровая гигиена»/ Министерство образования и науки Самарской области, 2019.
15. М.С. Наместникова. Информационная безопасность, или На расстоянии одного вируса. 7-9 классы/ М.: Просвещение, 2019

Цель:

- 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:

- сформировать общекультурные навыки работы с информацией (умения, связанные с поиском, пониманием, организацией, архивированием цифровой информации и ее критическим осмыслением, а также с 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 ответственного отношения 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.

II. Личностные и метапредметные, предметные результаты освоения курса внеурочной деятельности.

Личностные УУД:

- 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 понимания ценности безопасного образа жизни; интериоризация правил индивидуального и коллективного безопасного поведения в информационно-телекоммуникационной среде.

Метапредметные УУД:

Коммуникативные:

- строить позитивные отношения в процессе учебной и познавательной деятельности;
- критически относиться к собственному мнению, с достоинством признавать ошибочность своего мнения (если оно таково) и корректировать его;
- договариваться о правилах и вопросах для обсуждения в соответствии с поставленной перед группой задачей;
- делать оценочный вывод о достижении цели коммуникации непосредственно после завершения коммуникативного контакта и обосновывать его;
- целенаправленно искать и использовать информационные ресурсы, необходимые для решения учебных и практических задач с помощью средств ИКТ;
- 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.

Регулятивные:

- 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 и 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 в виде технологии решения практических задач определенного класса;

- оценивать свою деятельность, аргументируя причины достижения или отсутствия планируемого результата;
- находить достаточные средства для выполнения учебных действий в изменяющейся ситуации и/или при отсутствии планируемого результата;
- работая по своему плану, вносить коррективы в текущую деятельность на основе анализа изменений ситуации для получения запланированных характеристик продукта/результата;
- принимать решение в учебной ситуации и нести за него ответственность.

Познавательные:

- выделять явление из общего ряда других явлений;
- определять обстоятельства, которые предшествовали возникновению связи между явлениями, из этих обстоятельств выделять определяющие, способные быть причиной данного явления, выявлять причины и следствия явлений;
- строить рассуждение от общих закономерностей к частным явлениям и от частных явлений к общим закономерностям;
- излагать полученную информацию, интерпретируя ее в контексте решаемой задачи;
- самостоятельно указывать на информацию, нуждающуюся в проверке, предлагать и применять способ проверки достоверности информации;
- критически оценивать содержание и форму текста;
- определять необходимые ключевые поисковые слова и запросы.

Предметные:

- 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.
- приемами безопасной организации своего личного пространства данных с использованием индивидуальных накопителей данных, интернет-сервисов и т.п.
- основами соблюдения норм информационной этики и права;
- основами самоконтроля, самооценки, принятия решений и осуществления осознанного выбора в учебной и познавательной деятельности при формировании современной культуры безопасности жизнедеятельности;
- использовать для решения коммуникативных задач в области безопасности жизнедеятельности различные источники информации, включая Интернет-ресурсы и другие базы данных.

III. Содержание курса внеурочной деятельности с указанием срока реализации, количество часов в год, форм организации и видов деятельности.

Содержание программы учебного курса (Модуль 1) соответствует темам примерной основной образовательной программы основного общего образования (ПООП ООО) 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 ввести 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 4-6 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 с 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 проектов. 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 5 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.4 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. 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.5 Повторение. Волонтерская практика. 3 часа.

МЕТОДЫ РЕАЛИЗАЦИИ

- Репродуктивный – (беседа, вопросы)
- Проблемный
- Частично-поисковый – (творческие задания).
- Объяснительно-иллюстративный.

ФОРМЫ ЗАНЯТИЙ

Просматривание отрывков из познавательных, научно-популярных фильмов, видеоролики, рассматривание ситуативных иллюстраций, творческая работа, работа в группах.

Срок реализации программы: 1 год (34 часа).

IV. КАЛЕНДАРНО-ТЕМАТИЧЕСКОЕ ПЛАНИРОВАНИЕ ПО «ЦИФРОВОЙ ГИГИЕНЕ» В 7 КЛАССЕ

№ урока	Наименование раздела, тема урока	Кол- во часов	Форма проведения	Формы контроля	СОТ
Тема 1. «Безопасность общения» - 13 ч.					
1	Общение в социальных сетях и мессенджерах	1	Эвристическая беседа Групповая работа	Фронтальный опрос	Проблемное обучение
2	С кем безопасно общаться в интернете	1	Групповая работа	Фронтальный опрос	Исследовательский метод
3	Пароли для аккаунтов социальных сетей	1	Индивидуальная работа Тренинг	Сам.работа	Проблемное обучение Игровая технология
4	Безопасный вход в аккаунты	1	Индивидуальная работа	Сам.работа	Проблемное обучение
5	Настройки конфиденциальности в социальных сетях	1	Рассматривание ситуативных иллюстраций.	Работа в группах	Проблемный
6	Публикация информации в социальных сетях	1	Эвристическая беседа	Фронтальный опрос	Репродуктивный – (беседа, вопросы)
7	Кибербуллинг	1	Просматривание отрывков из познавательных, научно-популярных фильмов, видеоролики.	Фронтальный опрос	ИКТ Репродуктивный – (беседа, вопросы)
8	Публичные аккаунты	1	Эвристическая беседа Групповая работа	Работа в группах.	Проблемный
9-10	Фишинг	2	Эвристическая беседа Групповая работа	Работа в группах.	Проблемный
11-13	Выполнение и защита индивидуальных и групповых проектов	3	Исследование Групповая и индивидуальная работа	Разработка проекта	Проектный метод Обучение в сотрудничестве Частично-поисковый
Тема 2. «Безопасность устройств» - 8 ч.					
14	Что такое вредоносный код	1	Просматривание отрывков из познавательных, научно-популярных фильмов, видеоролики.	Фронтальный опрос	ИКТ Репродуктивный – (беседа, вопросы)
15	Распространение вредоносного кода	1	Просматривание отрывков из познавательных, научно-популярных фильмов, видеоролики.	Фронтальный опрос	ИКТ Репродуктивный – (беседа, вопросы)
16-17	Методы защиты от вредоносных программ	2	Эвристическая беседа Групповая работа	Работа в группах.	Проблемный
18	Распространение вредоносного кода для	1	Индивидуальная работа Групповая работа	Сам.работа	Частично-поисковый – (творческие задания).

	мобильных устройств				
19-21	Выполнение и защита индивидуальных и групповых проектов	3	Исследование Групповая и индивидуальная работа	Разработка проекта	Проектный метод Обучение в сотрудничестве Частично-поисковый
Тема 3 «Безопасность информации» - 14 ч.					
22	Социальная инженерия: распознать и избежать	1	Индивидуальная работа	Сам.работа	Обучение в сотрудничестве Исследовательский метод Частично-поисковый – (творческие задания).
23	Ложная информация в Интернете	1	Индивидуальная работа	Сам.работа	Частично-поисковый – (творческие задания). Проблемное обучение Игровая технология Разноуровневое обучение
24	Безопасность при использовании платежных карт в Интернете	1	Эвристическая беседа Групповая работа	Работа в группах	Репродуктивный – (беседа, вопросы) Проблемный Обучение в сотрудничестве
25	Беспроводная технология связи	1	Просматривание отрывков из познавательных, научно-популярных фильмов, видеоролики.	Фронтальный опрос Сам.работа	Репродуктивный – (беседа, вопросы) ИКТ
26	Резервное копирование данных	1	Индивидуальная работа Групповая работа	Сам.работа Работа в группах	Частично-поисковый – (творческие задания). Обучение в сотрудничестве
27-28	Основы государственной политики в области формирования культуры информационной безопасности	2	Просматривание отрывков из познавательных, научно-популярных фильмов, видеоролики.	Фронтальный опрос Сам.работа	Репродуктивный – (беседа, вопросы) Объяснительно-иллюстративный. ИКТ
29-31	Выполнение и защита индивидуальных и групповых проектов	3	Исследование Групповая и индивидуальная работа	Разработка проекта	Проектный метод Обучение в сотрудничестве Частично-поисковый
32-34	Повторение	3	Групповая работа Индивидуальная работа	Сам.работа Работа в группах	Репродуктивный Обучение в сотрудничестве Игровая технология