

муниципальное бюджетное общеобразовательное учреждение
«Школа № 165» городского округа Самара

«Рассмотрено»
на заседании УВЦ
Протокол № 1
Председатель УВЦ
Мамкина Н.В.
«25» 08 2022 г.

«Утверждаю»
Директор
МБОУ Школы №165 г.о.Самара
В.В. Дюлюкина
Приказ № 134
«26» 08 2022 г.

РАБОЧАЯ ПРОГРАММА
курса внеурочной деятельности, направленного на обеспечение благополучия
обучающихся в пространстве общеобразовательной школы
«Информационная безопасность»
(кружок)

5 - 9 класс

Рекомендовано
Координационным советом учебно –
методических объединений в системе
общего образования Самарской области
(протокол №27 от 21.08.2019г)
Министерства образования и науки
Самарской области

Пояснительная записка

При составлении данной программы авторами были использованы следующие нормативно-правовые и методические документы:

- Федеральный Закон от 29.12.2012 № 273-ФЗ «Об образовании в Российской Федерации» (ред. от 06.03.2019).
- Федеральный государственный образовательный стандарт основного общего образования, утвержденный приказом Министерства образования и науки Российской Федерации от 17.12.2010 № 1897 (в редакции приказа №1577 от 31.12.2015).
- Приказ Министерства просвещения Российской Федерации от 22.03.2021 N 115 «Об утверждении Порядка организации и осуществления образовательной деятельности по основным общеобразовательным программам - образовательным программам начального общего, основного общего и среднего общего образования».
- Постановление Главного Государственного врача Российской Федерации от 30.06.2020 №16 санитарно-эпидемиологические правила СП 3.1/2.4.3598-20 «Санитарно-эпидемиологические требования к устройству, содержанию и организации работы образовательных организаций и других объектов социальной инфраструктуры для детей и молодежи в условиях распространения новой коронавирусной инфекции (COVID-19)»
- Постановление Главного государственного санитарного врача Российской Федерации от 21.03.2022 № 9 "О внесении изменений в санитарно-эпидемиологические правила СП 3.1/2.4.3598-20 "Санитарно-эпидемиологические требования к устройству, содержанию и организации работы образовательных организаций и других объектов социальной инфраструктуры для детей и молодежи в условиях распространения новой коронавирусной инфекции (COVID-2019)", утвержденные постановлением Главного государственного санитарного врача Российской Федерации от 30.06.2020 № 16".
- Постановление Главного Государственного врача Российской Федерации от 28.09.2020 №28 Об утверждении санитарных правил СП 2.4.3648-20 «Санитарно-эпидемиологические требования к организациям воспитания и обучения, отдыха и оздоровления детей и молодежи».
- Постановление Главного государственного санитарного врача Российской Федерации от 28.01.2021 № 2 "Об утверждении санитарных правил и норм СанПиН 1.2.3685-21 "Гигиенические нормативы и требования к обеспечению безопасности и (или) безвредности для человека факторов среды обитания".
- Федеральный перечень учебников, утвержденный приказом Министерства просвещения Российской Федерации от 20.05.2020 №254 (с изменениями от 23.12.2020 №766)
- Приказ Минпросвещения России от 05.10.2020 №546 (с изменениями от 22.03.2021) «Об утверждении Порядка заполнения, учета и выдачи аттестатов об основном общем и среднем общем образовании и их дубликатов».

- Приказ министерства образования и науки Самарской области от 04.09.2014 № 276-ОД «Об утверждении Порядка регламентации и оформления отношений государственной и муниципальной образовательной организации, и родителей (законных представителей) обучающихся, нуждающихся в длительном лечении, а также детей-инвалидов, осваивающих основные общеобразовательные программы на дому, в Самарской области» (с изменениями от 10.08.2016г. №259-од)).
- Письмо министерства образования и науки Самарской области от 23.08.2016 № 815-ТУ «Об организации обучения на дому по основным общеобразовательным программам обучающихся, нуждающихся в длительном лечении, а также детей-инвалидов».
- Письмо Департамента государственной политики в сфере общего образования Минобрнауки России от 25.05.2015 № 08-761 «Об изучении предметных областей: «Основы религиозных культур и светской этики и «Основы духовно-нравственных культур и народов России».
- Письмо Минобрнауки России от 19.01.2018 №08-96 «О методических рекомендациях курса ОДНКНР».
- Письмо Рособрнадзора от 20.06.2018 №05-192 «О реализации прав на изучение родных языков народов РФ в общеобразовательных организациях».
- Письмо Минобрнауки России от 18.08.2017 №09-1672 «О направлении Методических рекомендаций по уточнению понятия и содержания внеурочной деятельности в рамках реализации основных общеобразовательных программ, в т.ч. в части проектной деятельности».
- Письмо Министерства образования науки Самарской области от 17.02.2016 №МО16-09-01/173-ту «О внеурочной деятельности»
- Устав МБОУ Школы № 165, Положение о формах, периодичности и порядке текущего контроля успеваемости и промежуточной аттестации, обучающихся МБОУ Школа № 165 г.о. Самара.
- ООП ООО МБОУ Школы № 165 г. о. Самара.

С каждым годом молодёжи в Интернете становится больше. Социальные сети входят в нашу жизнь, многие люди находятся там постоянно. Многие пользователи не понимают, что информация, размещенная ими в социальных сетях, может быть найдена и использована кем угодно, в том числе не обязательно с благими намерениями. И поэтому наша жизнь диктует новые требования как к организации самого учебно-воспитательного процесса в средней школе, так и к содержанию образования.

Актуальность

Новизна данной образовательной программы построена с учетом психологических особенностей подросткового возраста, опираясь на возрастающую тенденцию использования интернет ресурсов.

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 программы:

- 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 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.

Режим занятий. Программа внеурочной деятельности «Информационная безопасность» реализуется на базе МБОУ «Школа №165» г.о.Самара. Программа рассчитана на 68 часов (34 ч в год, 1 час в неделю). Возраст детей 12-15 лет, количество детей в группе до 25 человек.

Результаты освоения курса.

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

II. Метапредметные:

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:

- 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.

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.

III. Предметные (на конец освоения курса):

Обучающиеся научатся:

- 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.

Обучающиеся получают возможность научиться:

- 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.

IV. Воспитательные результаты:

Результаты первого уровня (приобретение социальных знаний, понимания социальной реальности и повседневной жизни):

- получение элементарных представлений о значении участия человека в общественно-полезной деятельности;
- приобретение начального опыта участия в различных видах общественно-полезной деятельности.

Формы достижения результатов первого уровня: познавательные беседы, инструктажи, социальные пробы, экскурсии, беседы о здоровом образе жизни. Формы контроля результатов первого уровня: мини-тренинги, листовки

Результаты второго уровня (получение опыта переживания и позитивного отношения к базовым ценностям общества): получение опыта позитивного отношения к общественно-полезной деятельности. Формы достижения результатов второго уровня: агитбригада, трудовые десанты, оздоровительные акции, социально-значимые акции. Формы контроля результатов второго уровня: экосубботники, акции.

Результаты третьего уровня (получение опыта самостоятельного общественного действия): потребность участия в общественно-полезной деятельности в окружающем школу социуме. Формы достижения результатов третьего уровня: исследовательские работы, социально-значимые акции в социуме (вне ОУ), краеведческие походы, конкурсы, слёты. Формы контроля результатов третьего уровня: просветительские экологические мероприятия, социально значимые мероприятия, слёты волонтеров

Содержание курса

Содержание программы учебного курса соответствует темам и основной образовательной программе основного общего образования 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 завершается выполнением проектной работы по одной из тем, предложенных на выбор учащихся и/или проверочного теста.

Безопасность общения.

Общение в социальных сетях и мессенджерах. Социальная сеть. История социальных сетей. Мессенджеры. Назначение социальных сетей и мессенджеров. Пользовательский контент.

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

Пароли для аккаунтов социальных сетей. Сложные пароли. Онлайн генераторы паролей. Правила хранения паролей. Использование функции браузера по запоминанию паролей.

Безопасный вход в аккаунты. Виды аутентификации. Настройки безопасности аккаунта. Работа на чужом компьютере с точки зрения безопасности личного аккаунта.

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

Публикация информации в социальных сетях. Персональные данные. Публикация личной информации.

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

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

Фишинг. 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.

9 класс.

Безопасность устройств.

Что такое вредоносный код. Виды вредоносных кодов. Возможности и деструктивные функции вредоносных кодов.

Распространение вредоносного кода. 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.

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

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

Безопасность информации.

Социальная инженерия: распознать и избежать. Приемы социальной инженерии. Правила безопасности при виртуальных контактах.

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

Безопасность при использовании платежных карт в Интернете. Транзакции и связанные с ними риски. Правила совершения онлайн покупок. Безопасность банковских сервисов.

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

Резервное копирование данных. Безопасность личной информации. Создание резервных копий на различных устройствах.

Основы государственной политики в области формирования культуры информационной безопасности. 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.

Тематическое планирование 8 класс

№	Раздел/тема	Кол-во часов
	Безопасность общения.	
1	Общение в социальных сетях и мессенджерах	5
2	С кем безопасно общаться в интернете	4
3	Пароли для аккаунтов социальных сетей	3
4	Безопасный вход в аккаунты	3
5	Настройки конфиденциальности в социальных сетях.	2
6	Публикация информации в социальных сетях	3
7	Кибербуллинг	2
8	Публичные аккаунты	3
9	Фишинг	4
10	Выполнение и защита индивидуальных проектов	5
	Итого:	34ч

9 класс

№	Раздел/тема	Кол-во часов
	Безопасность устройств.	
1	Что такое вредоносный код	3
2	Распространение вредоносного кода	4
3	Методы защиты от вредоносных программ	5
4	Распространение вредоносного кода для мобильных устройств.	2
	Безопасность информации.	
5	Социальная инженерия: распознать и избежать	2
6	Ложная информация в Интернете	3
7	Безопасность при использовании платежных карт в Интернете	3
8	Беспроводная технология связи	2
9	Резервное копирование данных	1
10	Основы государственной политики в области формирования культуры информационной безопасности	4
11	Выполнение и защита индивидуальных проектов	5
	Итого:	34ч