Государственное бюджетное общеобразовательное учреждение Самарской области средняя общеобразовательная школа «Образовательный центр» имени Героя Советского Союза Панчикова Василия Ивановича с.Богдановка муниципального района Нефтегорский Самарской области

ПРОВЕРЕНО
ио заместителя директора по УВР
_____Морозова И.В.
«31» августа 2022 г.

УТВЕРЖДАЮ
Директор ГБОУ СОШ с.Богдановка
_____ Е.М.Илясова
«31» августа 2022 г.

C=RU,
O=ГБОУ СОШ с.Богдановка,
CN=Директор Илясова Е.М.,
E=bogdan-school@mail.ru
009748439d494269a1
2022.10.28 21:32:11+03'00'

РАБОЧАЯ ПРОГРАММА

курса внеурочной деятельности

Интернет-безопасность

Класс: 7-8

Составитель:
И.Б.Куленко
учитель информатики
ГБОУ СОШ с.Богдановка

РАССМОТРЕНА
на заседании МО учителей
естественно-научного цикла
Протокол № 1 от 30.08.2022 г
Руководитель МО
_____ И.В. Морозова

ПОЯСНИТЕЛЬНАЯ ЗАПИСКА

Рабочая программа составлена на основе следующих документов:

1. Федеральный Закон от 29.12.2012 г. № 273-ФЗ «Об образовании в Российской Федерации».
2. Федеральный государственный образовательный стандарт основного общего образования (ФГОС ООО).
3. Основная образовательная программа основного общего образования ГБОУ СОШ с. Богдановка.
4. Примерная рабочая программа учебного курса «Цифровая гигиена» (7-9 классы) (рекомендованная координационным советом УМО в системе общего образования СО, 2019 г.)

Программа курса «Интернет-безопасность» адресована учащимся 7 и 8 классов, а также родителям обучающихся всех возрастов и учитывает требования, выдвигаемые федеральным государственным образовательным стандартом основного общего образования к предметным (образовательные области «Математика и информатика», «Физическая культура и основы безопасности жизнедеятельности»), метапредметным и личностным.

Изучение курса «Интернет-безопасность» в основной школе направлено на достижение следующих **целей:**

- 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).

Основными **задачами** реализации содержания курса являются:

- 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.

Актуальность программы: формирование у школьников навыков эффективного поведения в сети Интернет - новая и крайне актуальная педагогическая задача. На современном этапе развития общества ведущая роль закрепилась за информационной сферой. Средства массовой информации (СМИ) и коммуникации (СМК) приобрели значение мощнейших воспитательных сил. Они закладывают ценности и жизненные ориентации, формируют мировоззрение современных детей и подростков, порой преобладая над воздействием, оказываемым таким воспитательным институтом как семья. Интернет стал неотъемлемой частью жизни человека и количество детей- пользователей неуклонно растет. Современные дети используют кардинально другие инструменты и способы получения информации, принципиально другие системы коммуникации. Окружающая их смешанная реальность не может не влиять на когнитивное и личностное развитие ребенка. Вместе с тем все более актуальными становятся вопросы интернет-безопасности, так как стремительное овладение Интернетом детьми и подростками сопряжено с их недостаточной осведомленностью как о рисках и угрозах цифрового мира, так и и о возможностях совладания с ними. Деструктивные установки, кибербуллинг и кибермоббинг, интернет-мошенничества, группы смерти в социальных сетях и

другой негативный контент – лишь небольшая часть интернет-угроз, которые могут негативно воздействовать на несовершеннолетнего пользователя. Обеспечение психологической безопасности ребенка и подростка в интернете является важнейшей задачей информационного общества, во многом это задача семейного и школьного воспитания. В Национальной стратегии действий в интересах детей, определяющем основные направления государственной политики в сфере защиты детства, зафиксировано, что акцент должен быть на создании и внедрении программ обучения детей и подростков правилам безопасного поведения в интернет-пространстве, а также профилактике интернет-зависимости. Причем новые федеральные государственные образовательные стандарты (ФГОС) предусматривают формирование навыков безопасного использования Интернета не только в рамках таких образовательных программ, как информатика, обществознание, право, основы безопасности жизнедеятельности, но также в рамках программ внеурочной деятельности, в рамках программ воспитания и социализации, являющихся неотъемлемой частью основного образовательного курса

Данная рабочая программа может быть реализована как для детей, обучающихся по общеобразовательной программе, так и для обучающихся с ограниченными возможностями здоровья (ОВЗ). Получение образования детьми особой категории является необходимым условием их успешной социализации, обеспечения полноценного участия в жизни общества, эффективной самореализации в различных видах профессиональной и социальной деятельности. Для обучающихся с ОВЗ программа реализуется с учетом особенностей их психофизического развития, индивидуальных возможностей, обеспечивающая коррекцию нарушений развития и социальную адаптацию.

Общая характеристика учебного курса

Курс «Интернет-безопасность» 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.

Отбор тематики содержания курса осуществлен с учетом целей и задач ФГОС основного общего образования, возрастных особенностей и познавательных возможностей обучающихся 8 классов. Рекомендуется для реализации в рамках внеурочной деятельности обучающихся.

В преподавании курса 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 профилактики 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, практические работы и т.д.).

Место курса в учебном плане

На изучение курса «Интернет-безопасность» отводится по 1 часу в неделю в 7 и 8 классах. Программа рассчитана на 34 учебных часа (34 учебные недели) в год.

I. РЕЗУЛЬТАТЫ ОСВОЕНИЯ КУРСА

Личностные, метапредметные и предметные результаты освоения содержания курса

Программа курса обеспечивает достижение выпускниками основной школы комплекса личностных, метапредметных и предметных результатов.

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 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 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 универсальные учебные действия.

В результате освоения учебного курса обучающийся сможет:

- 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.

Коммуникативные универсальные учебные действия.

В результате освоения учебного курса обучающийся сможет:

- 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.

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

II. СОДЕРЖАНИЕ КУРСА

Раздел 1. «Безопасность общения»

Тема 1. Общение в социальных сетях и мессенджерах. Социальная сеть. История социальных сетей. Мессенджеры. Назначение социальных сетей и мессенджеров. Пользовательский контент.

Тема 2. 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.

Тема 3. Пароли для аккаунтов социальных сетей. Сложные пароли. Онлайн генераторы паролей. Правила хранения паролей. Использование функции

браузера по запоминанию паролей.

Тема 4. Безопасный вход в аккаунты. Виды аутентификации. Настройки безопасности аккаунта. Работа на чужом компьютере с точки зрения безопасности личного аккаунта.

Тема 5. Настройки конфиденциальности в социальных сетях. Настройки приватности и конфиденциальности в разных социальных сетях. Приватность и конфиденциальность в мессенджерах.

Тема 6. Публикация информации в социальных сетях. Персональные данные. Публикация личной информации.

Тема 7. Кибербуллинг. Определение кибербуллинга. Возможные причины кибербуллинга и как его избежать? Как не стать жертвой кибербуллинга. Как помочь жертве кибербуллинга.

Тема 8. Публичные аккаунты. Настройки приватности публичных страниц. Правила ведения публичных страниц. Овершеринг.

Тема 9. 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.

Раздел 2. «Безопасность устройств»

Тема 1. Что такое вредоносный код. Виды вредоносных кодов. Возможности и деструктивные функции вредоносных кодов.

Тема 2. 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.

Тема 3. Методы защиты от вредоносных программ. Способы защиты устройств от вредоносного кода. Антивирусные программы и их характеристики. Правила защиты от вредоносных кодов.

Тема 4. Распространение вредоносного кода для мобильных устройств. Расширение вредоносных кодов для мобильных устройств. Правила безопасности при установке приложений на мобильные устройства.

Выполнение и защита индивидуальных и групповых проектов.

Раздел 3 «Безопасность информации»

Тема 1. Социальная инженерия: распознать и избежать. Приемы социальной инженерии. Правила безопасности при виртуальных контактах.

Тема 2. Ложная информация в Интернете. Цифровое пространство как площадка самопрезентации, экспериментирования и освоения различных социальных ролей. Фейковые новости. Поддельные страницы.

Тема 3. Безопасность при использовании платежных карт в Интернете. Транзакции и связанные с ними риски. Правила совершения онлайн покупок. Безопасность банковских сервисов.

Тема 4. Беспроводная технология связи. Уязвимость Wi-Fi-соединений. Публичные и непубличные сети. Правила работы в публичных сетях.

Тема 5. Резервное копирование данных. Безопасность личной информации. Создание резервных копий на различных устройствах.

Тема 6. 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.

Пособия и обучающие программы по формированию навыков цифровой гигиены.

Выполнение и защита индивидуальных и групповых проектов. 3 часа.

III. ТЕМАТИЧЕСКОЕ ПЛАНИРОВАНИЕ

№	Тема занятия	Всего часов	Теория	Практика	Формы деятельности
	Тема 1. «Безопасность общения»				
1	Общение в социальных сетях и мессенджерах	1	1	0	Беседа
2	С кем безопасно общаться в интернете	1	0,5	0,5	Беседа, круглый стол.
3	Пароли для аккаунтов социальных сетей	1	0,5	0,5	Квест, дискуссия.
4	Безопасный вход в аккаунты	1	0	1	Практикум.
5	Настройки конфиденциальности в социальных сетях	1	0	1	Практикум.
6	Публикация информации в социальных сетях	1	1	0	Учебный диалог
7	Кибербуллинг	1	1	0	Беседа
8	Публичные аккаунты	1	0	1	Исследовательская работа, практикум.

9-10	Фишинг	2	1	1	Беседа, обсуждение, практикум.
11-13	Выполнение и защита индивидуальных и групповых проектов	3	1	2	Работа в парах
Тема 2. «Безопасность устройств»					
14	Что такое вредоносный код	1	0,5	0,5	Презентация, беседа.
15	Распространение вредоносного кода	1	1	0	Развивающая игра
16-17	Методы защиты от вредоносных программ	2	1	1	уждение, урок-исследование.
18	Распространение вредоносного кода для мобильных устройств	1	0	1	Практикум
19-21	Выполнение и защита индивидуальных и групповых проектов	3	1	2	Работа в парах
Тема 3 «Безопасность информации»					
22	Социальная инженерия: распознать и избежать	1	0,5	0,5	Презентация.
23	Ложная информация в Интернете	1	0,5	0,5	Мини-проект
24	Безопасность при использовании платежных карт в Интернете	1	1	0	Изучение информации
25	Беспроводная технология связи	1	1	0	Задание исследовательского характера
26-27	Резервное копирование данных	2	1	1	Обсуждение. Исследование. Проектная работа.
28-29	Основы государственной политики в области формирования культуры информационной безопасности	2	1	1	Учебный диалог
30-31	Пособия и обучающие программы по формированию навыков цифровой гигиены.	2	0,5	1,5	Исследовательская работа, урок-практикум.
32-34	Выполнение и защита индивидуальных и групповых проектов	3	1	2	Работа в парах