Муниципальное общеобразовательное учреждение
«Средняя школа № 26»

Принята на заседании
Педагогического совета
« 07 » июня 2023 г.
Протокол № 10

УТВЕРЖДАЮ:
Директор _____
« 07 » июня 2023 г.

Дмитриева Любовь Валентиновна
Подписано цифровой подписью: Дмитриева Любовь Валентиновна
Дата: 2023.08.24 13:47:05 +03'00'

Дополнительная общеобразовательная общеразвивающая программа
естественнонаучной направленности

Безопасность в сети Интернет

Возраст обучающихся: 11 – 17 лет
Срок реализации: 1 год

Автор-составитель:
Калина Е.А., ПДО

г. Ярославль, 2023 г.

Содержание

Раздел 1. Пояснительная записка

Дополнительная общеобразовательная общеразвивающая программа «Безопасность в сети Интернет» (далее программа) составлена в соответствии со следующими нормативно-правовыми документами:

- Федеральный закон от 29.12.12 г. № 273-ФЗ «Об образовании в Российской Федерации»;
- Приказ Министерства образования и науки Российской Федерации (Минобрнауки России) от 09 ноября 2018 г. № 196 г. Москва «Об утверждении Порядка организации и осуществления образовательной деятельности по дополнительным общеобразовательным программам»;
- Концепция развития дополнительного образования детей до 2030 года и плана мероприятий по ее реализации (Распоряжение Правительства РФ от 31 марта 2022 г. N 678-р);
- Стратегия развития воспитания в Российской Федерации на период до 2025 года, утвержденной распоряжением Правительства от 29.05.2015 № 996-р;
- Санитарные правила СП 2.4.3648-20 «Санитарно-эпидемиологические требования к организации воспитания и обучения, отдыха и оздоровления молодежи», утвержденные 28.09.2020 (Постановление № 28 Главного государственного санитарного врача РФ);
- Приказ департамента образования Ярославской области от 07.08.2018 № 19-нп «Об утверждении Правил персонифицированного финансирования дополнительного образования детей в Ярославской области»
- Устав ОО

Дополнительная общеобразовательная общеразвивающая программа «Безопасность в сети Интернет» разработана в связи с возросшей потребностью обеспечения информационной безопасности детей и подростков. Программа разработана для следующих уровней общего образования: основного общего и среднего общего образования.

Направленность дополнительной общеобразовательной программы - естественнонаучная.

Исследование проблемы безопасности детей и подростков в сети Интернет последние годы является особенно **актуальным,** в связи с бурным

развитием IT- технологий и со свободным использованием детьми и подростками современных информационно - коммуникационных технологий (Интернет, сотовая (мобильная) связь).

Программа разработана с учетом требований законов Российской Федерации: «Об образовании в Российской Федерации», «О защите детей от информации, причиняющей вред их здоровью и развитию» и «Санитарно-эпидемиологических требований к условиям и организации обучения в общеобразовательных учреждениях» и "Санитарно- эпидемиологических требований к устройству, содержанию и организации режима работы образовательных организаций дополнительного образования детей".

Новизна состоит в том, что общеобразовательная общеразвивающая программа «Безопасность в сети Интернет» способствует формированию навыков и умений безопасного и целесообразного поведения при работе с компьютерными программами и в сети интернет, умению соблюдать нормы информационной этики и права.

Цель программы: освоение обучающимися базовых принципов безопасного поведения в сети интернет и безопасности личного информационного пространства.

Задачи обучения:

Образовательные:

1. Способствовать формированию знаний о безопасном поведении при работе скомпьютерными программами, информацией в сети Интернет;
2. Формировать умения соблюдать нормы информационной этики;
3. Формировать умения безопасной работы с информацией, анализировать иобобщать полученную информацию.

Развивающие:

1. Развивать компьютерную грамотность информационную культуру личности в использовании информационных и коммуникационных технологий;
2. Развивать умение анализировать и систематизировать имеющуюся информацию;
3. Развивать познавательную и творческую активность в безопасном использованииинформационных и коммуникационных технологий;

Воспитательные:

1. Способствовать выработке сознательного и бережного отношения к вопросамсобственной информационной безопасности;
2. Способствовать формированию и развитию нравственных, этических,патриотических качеств личности.
3. Стимулировать поведение и деятельность, направленные на соблюдениеинформационной безопасности.

Контингент обучаемых: программа рассчитана для обучающихся по двум уровням образования (основное общее образование, среднее общее образование). Объемом 34 часа.

5, 10 и 11 класс – по 9 часов

6, 7, 8, 9 класс – по 8 часов

Данная программа составлена на основе курса «Основы кибербезопасности» для общеобразовательных организаций авторов Тонких И.М., Комарова М.М., Ледовского В.И., Михайлова А.В., переработана и модифицирована.

Содержание программного материала этих тем, как в теории, так и на практических занятиях составлено с учётом возрастных особенностей обучающихся, весь материал построен по принципу от простого к сложному.

Практические работы в содержании программы возможно использовать в качестве вариативных, индивидуальных практических заданий разного уровня углубленности, доступности и степени сложности исходя из диагностики и стартовых возможностей каждого из участников рассматриваемой программы.

Планируемые результаты:

Предметные:

1. Сформированы знания о безопасном поведении при работе с компьютерными программами, информацией в сети интернет;
2. Сформированы умения соблюдать нормы информационной этики;
3. Сформированы умения безопасно работать с информацией, анализировать и обобщать полученную информацию.

Метапредметные:

1. Развиваются компьютерная грамотность и информационная культура личности в использовании информационных и коммуникационных технологий;
2. Развиваются умения анализировать и систематизировать имеющуюся информацию;
3. Развиваются познавательная и творческая активность в безопасном использовании информационных и коммуникационных технологий.

Личностные:

1. Вырабатывается сознательное и бережное отношение к вопросам собственной информационной безопасности;
2. Формируются и развиваются нравственные, этические, патриотические качества личности;
3. Стимулируется поведение и деятельность, направленные на соблюдение информационной безопасности.

Режим занятий -занятия по данной программе - один раз в неделю в школе в соответствии с нормами СанПиН 2.4.2.2821-10 или СанПиН 2.4.4.3172-14.

Формы проведения занятий:

Формы организации деятельности: групповая. Занятия проводятся в комбинированной, теоретической и практической форме:

- теоретические занятия: основы безопасного поведения при работе с компьютерными программами, информацией в сети интернет, изучение терминов, беседы,лекции;
- практические занятия: работа с мобильными устройствами; закупки в интернет магазине; квесты; создание буклетов и мультимедийных презентаций.

Раздел 2. Учебно-тематический план

№ п/п	Наименование раздела, тем	Класс	Количество часов	Из них	
				теория	практика
1	**Общение в сети Интернет и сетевой этикет**	5	6	3	3
2	**Риски в сети Интернет**	6	5	2	3
3	**Новостная грамотность в киберпространстве**.	5, 6,	3	2	1
4	**Интернет – зависимость**	7, 8	5	3	2
5	**Мошеннические действия в Интернете. Киберпреступления**	9, 10, 11	5	4	1
6	**Агрессия в сети и ее виды**	7, 8	4	2	2
7.	**Троллинг в киберпространстве**	10	3	2	1
8.	**Хейтинг: способы нейтрализации**	11	3	2	1
Итого:			34	20	14

Раздел 3. Содержание

Тема 1. Общение в сети Интернет и сетевой этикет. (6 часов)

Основные вопросы: Почему соцсети стали настолько популярными? Механизмы Интернет – общения. Графическая модель типов пользователей социальных сетей

Первая и главная причина – популяризация интернета. Именно с появлением подключения к Всемирной паутине в каждом доме соцсети стали одним из главных способов связи. Человечество всегда привлекала возможность коммуникации на расстоянии: телеграфы, телефоны, интернет.

Вторая причина – расширенный функционал. Социальные сети обладают не только возможностью переписываться и делиться новостями, но и:

- общаться по аудио- и видеосвязи;
- слушать музыку;
- смотреть фильмы, передачи, видео;
- делиться фотографиями;
- объединяться в сообщества по интересам;
- создавать коммерческие проекты и онлайн-представительства;
- вести бизнес, продавать товары и услуги;
- давать рекламу и многое другое.

Третья причина – физиология человека.

Механизмы Интернет – общения.

Анонимность (человек в сети может проявлять и проявляет большую свободу высказываний и поступков (вплоть до нецензурных выражений), так как риск разоблачения минимален)

Своеобразие протекания процессов межличностного восприятия в условиях отсутствия невербальной информации (сильное влияние на представление о собеседнике имеют механизмы стереотипизации и идентификации, а также установка желаемых качеств в партнере)

Добровольность и желательность контактов (пользователь Интернета добровольно завязывает всевозможные контакты или уходит от них, а также может прервать их в любой момент)

Затрудненность эмоционального компонента общения (стойкое стремление к эмоциональному наполнению текста, которое выражается в создании смайликов для обозначения эмоций)

Стремление к ненормативному поведению (пользователи проигрывают нереализуемые в деятельности вне сети роли, сценарии ненормативного поведения.

Требования к знаниям и умениям:

Обучающиеся должны знать популяризация интернета. Почему соцсети стали настолько популярными? Механизмы Интернет – общения.
Обучающиеся должны уметь различать графическая модель типов

пользователей социальных сетей. Обучающиеся должны уметь использовать этические и правовые нормы информационной деятельности человека, информационный этикет и право, информационную безопасность

Тематика практических работ:

Практическая работа. Составить информационный буклет «Моя безопасная сеть», создать групповую газету «Безопасность в Интернет», «Упражнение Интернет общение глазами ребят».

Тема № 2. (5 часов) Риски в сети Интернет.

Основные вопросы: риски в сети Интернет.

Обучающиеся должны знать: Контентные риски. Различные информационные ресурсы (тексты, картинки, аудио, видеофайлы, ссылки на сторонние ресурсы), содержащие противозаконную, неэтичную и вредоносную информацию. Коммуникационные риски связаны с общением и межличностными отношениями Интернет-пользователей. Электронные риски – это вероятность столкнуться с хищением персональной информации или подвергнуться атаке вредоносных программ. Потребительский риск заключается в потере денег без приобретения товара или приобретения товара низкого качества. Психологические риски интернет-зависимости.

Требования к знаниям и умениям:

Обучающиеся должны уметь различать риски в сети Интернет.

Тематика практических работ:

Практическая работа. Групповая работа «Риски в сети Интернет»

Создание буклета «Риски в сети Интернет».

Тема № 3. (3 часов)

Новостная грамотность в киберпространстве

Основные вопросы: Новостная грамотность. *Новость* - не жанр журналистского произведения, а новый фрагмент реальности, меняющий привычный ход вещей и потому требующий в той или иной степени общественного внимания. Виды новостей: *«Жесткая» новость, «Мягкая» новость, инфотейнмент, финишинг*. Главное, чтобы поднятая проблема была доведена до конца, закрыта в плане ее практического решения. Причем при использовании этого приема допускается повтор какой-то ситуации, факта, картинки, вопроса и т. д. Как оценить достоверность новостной информации? Как проверять информацию и не оказаться жертвой fake news? Принципы распознавания fake news. *Принцип первый:* проверьте площадку. *Принцип второй:* проверьте источники. *Принцип третий:* пускайте в свою голову только настоящих экспертов. *Принцип четвертый:* чем больше труда, тем лучше. *Принцип пятый:* ищите и распространяйте добавленную стоимость.

Требования к знаниям и умениям:

Обучающиеся должны знать новостную грамотность, виды новостей, как оценить достоверность новостной информации? Принципы распознавания

fake news.

Тематика практических работ:

Практическая работа. «Создание мультимедийной презентации «Осторожно фейк!».

Тема № 4. (5 часов)
Интернет зависимость

Основные вопросы: Термин "Интернет-зависимость" Термин "Интернет-зависимость" еще в 1996 году предложил доктор Айвен Голдберг для описания неоправданно долгого, возможно патологического, пребывания в Интернете. Виды интернет-зависимостей. Киберотношения. Зависимость от дружеских отношений, завязанных в комнатах общения, интерактивных играх и конференциях, которая заменяет реальных друзей и семью. Чрезмерная сетевая вовлеченность. Включает в себя вовлечение в азартные сетевые игры, зависимость от интерактивных аукционов и навязчивое состояние продавать и покупать через сеть. Информационная перегрузка и как ее опознать. Компьютерная зависимость. На сегодняшний день игровая зависимость официально признана врачами всего мира психическим заболеванием и включена в Международную классификацию болезней. Последствия компьютерной зависимости. *Физиологические проблемы:* Нарушение осанки; Рассеивается внимание; Снижаются умственные способности; Ухудшается память и зрение; Бессонница и потеря аппетита.

Требования к знаниям и умениям:

Обучающиеся должны знать виды интернет-зависимостей. Киберотношения. Информационная перегрузка и как ее опознать. Компьютерная зависимость и ее последствия.

Тематика практических работ:

Практическая работа. Создание презентации на тему: «Информационная перегрузка». Эссе «Я и Интернет»

Тема № 5. (5 часов)
Мошеннические действия в Интернете. Киберпреступления.

Основные вопросы: Виды интернет - мошенничества (письма, реклама, охота за личными данными и т.п.). Фишинг (фарминг). Мошеннические действия в сети. Предложения о разблокировании программ (блокировщики windows). Ложные антивирусы. Сбор «пожертвований» на благотворительность. «Легкий заработок» в Интернете. Пирамиды. Мошенничество при распространении «бесплатного» ПО. Продажа «обучающих курсов» для бизнеса. Опасности мобильной связи. Предложения по установке вредоносных приложений. Мошеннические СМС. Прослушивание разговоров. Определение местоположения телефона. Азартные игры. Онлайн - казино. Букмекерские конторы. Предложения для «инвестирования» денег. Выигрыш в лотерею. Технологии манипулирования в

Интернете. Техника безопасности при интернет-общении.

Требования к знаниям и умениям:

Обучающиеся должны знать: виды интернет-мошенничества, опасности мобильной сети, технику безопасности при регистрации на веб-сайтах, сайтах знакомств, понятия компьютерное пиратство, плагиат, кибернаемники и кибердетективы.

Обучающиеся должны уметь обезопасить себя при интернет-общении.

Тематика практических работ:

Практическая работа. Круглый стол «Как не стать жертвой сетевых шуток и розыгрышей».

Тема № 6. (4 часа)
Агрессия в сети и ее виды

Основные вопросы: Термины «Агрессия и агрессивность»

Если вы стали жертвой компьютерной агрессии: службы помощи личное общение и общение в группе – чем они отличаются (чаты, форумы, службы мгновенных сообщений). Киберагрессия (оскорбление, унижение, манипуляция, буллинг в интернет-среде) — ситуация, в которую, по статистике, в России регулярно вовлекается каждый пятый подросток. С размытием границ реального и виртуального киберагрессия оказывает не менее пагубное влияние на эмоциональное и психологическое здоровье детей, чем реальная травля в школе (и одно нередко перетекает в другое). Кибербуллинг. Признаки кибербуллинга – осознанное и длительное причинение человеку вреда в сети. При этом агрессоров может быть несколько, они выступают как от своего лица, так и анонимно.

Требования к знаниям и умениям:

Обучающиеся должны знать термины «Агрессия и агрессивность». Кибербуллинг. Признаки кибербуллинга. Обучающиеся должны уметь использовать этические и правовые нормы информационной деятельности человека.

Тематика практических работ:

Практическая работа. Круглый стол «Моя киберагрессия»

Тема №7. (3 часов)
Троллинг в киберпространстве

Основные вопросы: *Тро́ллинг* — форма социальной провокации или издевательства в сетевом общении, использующаяся как персонифицированными участниками, заинтересованными в большей узнаваемости, публичности, эпатаже, так и анонимными пользователями. Виды троллинга: обычная провокация; преднамеренная провокация; целенаправленная провокация; троллинг по заказу. Типы троллей: эмоциональный тролль; тролль-оффтопикт; тролль-борец за справедливость; тролль — любитель спойлеров; тролли-всезнайки; «Бессмысленные» тролли.;

«Актуальные» тролли; жестокие тролли.

.

Требования к знаниям и умениям:

Обучающиеся должны знать термит «Троллинг», его виды и типы. Обучающиеся должны уметь распознать троллинг и его виды в сети Интернет.

Тематика практических работ:

Практическая работа Беседа. Видео ролик: «Не кормите Провокатора. Тролли в Интернете».

Тема №8. (3 часов)
Хейтинг: способы нейтрализации

Основные вопросы: Хейтинг — это такой вид социальной активности. Хейтерами обычно называют людей, которые по злому насмехаются или поливают грязью в интернете. Злые комменты, едкие выражения в адрес кого-либо. На этом многие даже себе сделали имя. Некоторые хейтеры причисляют себя к критикам, но критика по крайней мере имеет какой-то конструктив. Виды хейтеров: «Правдоруб»; «Белое пальто»; «Тролль обыкновенный»; «Эффект Шарикова». Если вы понимаете мотивы поведения хейтера, то вы можете защищаться и атаковать его.

Требования к знаниям и умениям:

Обучающиеся должны знать термит «Хейтинг», его виды. Обучающиеся должны уметь распознать хейтинг и его виды в сети Интернет.

Тематика практических работ:

Практическая работа. Беседа. Видео ролик: «Хейтинг: способы нейтрализации».

Раздел 4. Обеспечение образовательной программы

Материально-техническое обеспечение курса «Безопасность в сети Интернет» включает следующий перечень необходимого оборудования:

№ п	**Наименование объектов и средств материально-технического обеспечен**	**Дидактическое описани**	**Обеспеченность, %**
СРЕДСТВА ИКТ			
1.	ПК	Используется учителем и учащимися	100
2.	Мультимедийный проектор.	Используется учителем	100
3.	Интерактивная доска.	Используется учителем и учащимися	100
4.	Доступ к сети Интернет.	Используется учителем и учащимися	100

Раздел 5. Оценка эффективности программы

Способы определения планируемых результатов – педагогическое наблюдение, тесты, педагогический анализ результатов анкетирования, тестирования, опросов, выполнения обучающимися диагностических заданий, участия в мероприятиях, решения задач поискового характера, активности обучающихся на занятиях и т.п.

Формами подведения итогов реализации дополнительной общеобразовательной программы «Безопасность в сети Интернет» могут быть выставки буклетов, конкурс презентаций, видео роликов выполненных обучающимися; проведение квестов; выступления обучающихся по актуальным вопросам информационной безопасности с собственными мультимедийными презентациями на ученических мероприятиях.

Раздел 6. Список используемой литературы.

- Бирюков А.А. Информационная безопасность защита и нападение 2- е издание: Издательство: ДМК-Пресс., 2017, 434 с.
- Бирюков А.А. Информационная безопасность защита и нападение.: Издательство: ДМК-Пресс., 2018, 474 с.
- Колесниченко Денис. Анонимность и безопасность в интернете. От чайника к пользователю. Самоучитель Издательство: БХВ-Петербург, 2018, 240с.
- Мазаник Сергей. Безопасность компьютера. Защита от сбоев, вирусов и неисправностей: издательство: ЭКСМО, 2019, 256 с.
- Мэйволд Э. Безопасность сетей (2-е изд.) Книги» Сетевые Технологии. Название: Безопасностьсетей: Издательство: М.: НОУ "Интуит", 2020,571 с.
- Платонов В.В. Программно-аппаратные средства защитыинформации: учебник для студ. Учрежд.высш.проф. образования / В. В.Платонов. — М.: Издательский центр «Академия», 2018, 336 с.
- Проскурин В.Г Защита в операционных системах: Издательство: Горячая линия-Телеком, 2019, 192 с.
- Савченко Е. Кто, как и зачем следит за вами через интернет: Москва - Третий Рим, 2019, 100 с.
- Яковлев В.А.Шпионские и антишпионские штучки: Техническая литература Издательство: Наука и Техника, 2018, 320 с.