Муниципальное бюджетное общеобразовательное учреждение
«Средняя общеобразовательная школа №1
с углубленным изучением отдельных предметов»

Утверждена
приказом директора
МБОУ «СОШ № 1 с углубленным изучением отдельных предметов»
от 30 августа 2023 г. № 01-08/169

Рабочая программа учебного курса внеурочной деятельности «Информационная безопасность»

для 5-9 классов, срок реализации 2023-2028,
основного общего образования

Составители:
Удовиков О.А.,
учитель иностранного языка .

г. Великий Устюг

ПОЯСНИТЕЛЬНАЯ ЗАПИСКА

Исследование проблемы безопасности детей и подростков в сети Интернет последние годы является особенно актуальным, в связи с бурным развитием ITтехнологий и со свободным использованием детьми и подростками современных информационно - коммуникационных технологий (Интернет, сотовая (мобильная) связь). Дополнительная общеобразовательная программа «Безопасность в сети Интернет» разработана в связи с возросшей потребностью обеспечения информационной безопасности детей и подростков при организации урочной и внеурочной деятельности. Программа разработана для основного общего уровня образования. Направленность дополнительной общеобразовательной программы - естественнонаучная. 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".

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 с компьютерными программами, информацией в сети Интернет; 2. Формировать умения соблюдать нормы информационной этики; 3 3. Формировать умения безопасной работы с информацией, анализировать и обобщать 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 использовании информационных и коммуникационных технологий.

Воспитательные: 1. Способствовать выработке сознательного и бережного отношения к вопросам собственной информационной безопасности; 2. Способствовать формированию и развитию нравственных, этических, патриотических качеств личности. 3. Стимулировать поведение и деятельность, направленные на соблюдение информационной безопасности.

Объем программы 34 часа. 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 проводятся один раз в неделю в рамках внеурочной деятельности.

Форма проведения занятий - 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.

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

Формы подведения итогов реализации данной дополнительной общеобразовательной программы могут быть выставки буклетов, выполненных обучающимися; проведение квестов; выступления обучающихся по актуальным вопросам информационной безопасности с собственными мультимедийными презентациями на ученических мероприятиях; демонстрация созданных видеороликов и др.

ТЕМАТИЧЕСКИЙ ПЛАН

№	Тема занятия	Всего часов	Теор. зан.	Практ. зан.
1	Общие сведения о безопасности ПК и Интернета	5	4	1
2	Техника безопасности и экология	5	4	1
3	Проблемы Интернет-зависимости	5	4	1
4	Методы обеспечения безопасности ПК и Интернета. Вирусы и антивирусы	5	4	1
5	Мошеннические действия в Интернете. Киберпреступления.	5	4	1
6	Сетевой этикет. Психология и сеть.	5	4	1
7	Государственная политика в области кибербезопасности.	4	4	0
	Итого:	34	28	6

СОДЕРЖАНИЕ ПРОГРАММЫ

Тема № 1. (5 часов)
Общие сведения о безопасности ПК и Интернета

1. Основные вопросы: Как устроены компьютер и интернет. Как работают мобильные устройства. Угрозы для мобильных устройств. Защита персональных данных, почему она нужна. Категории персональных данных. Биометрические персональные данные. Безопасный профиль в социальных сетях. Составление сети контактов. Защита киберпространства как комплекс мероприятий, направленных на обеспечение информационной безопасности. Аспекты кибербезопасности Компьютерная и информационная безопасность, обнаружение проблем сети, восстановление параметров систем, средства защиты от несанкционированного доступа к данным, криптографическая защита информации. Основные угрозы безопасности информации: утечки, потеря целостности, нарушение работоспособности системы, незаконное тиражирование (воспроизведение). Безопасный серфинг. Безопасные ресурсы для поиска.
2. Требования к знаниям и умениям: Обучающиеся должны знать как устроен компьютер и интернет, как работают мобильные устройства, какие существуют угрозы для мобильных устройств, что такое защита персональных данных, аспекты кибербезопасности, что такое компьютерная и 12 информационная безопасность, что такое кибертерроризм и кибервойны, основные угрозы безопасности информации. Обучающиеся должны уметь защищать свои персональные данные, составлять безопасные сети контактов, своевременно обнаружить проблемы сети, восстанавливать параметры систем.
3. Тематика практических работ: 1. Практическая работа. Составить информационный буклет «Моя безопасная сеть» или сделать групповую газету «Безопасность в Интернет».

Тема № 2. (5 часов)
Техника безопасности и экология

1. Основные вопросы: Правила поведения в компьютерном классе. Техника безопасности при работе с компьютером. Компьютер и мобильные устройства в чрезвычайных ситуациях. Компьютер и зрение. Воздействие радиоволн на

здоровье и окружающую среду (Wi-Fi, Bluetooth, GSM). Комплекс упражнений при работе за компьютером. Гигиена при работе с ПК

2. Требования к знаниям и умениям: Обучающиеся должны знать правила поведения в компьютерном классе, как применяются компьютер и мобильные устройства в чрезвычайных ситуациях, какое влияние оказывает компьютер на зрение, какое воздействие оказывают радиоволны на здоровье человека и окружающую среду. Обучающиеся должны уметь соблюдать требования ТБ при работе с компьютером, соблюдать гигиенические требования, проводить комплекс упражнений при работе за компьютером.

3. Тематика практических работ: Практическая работа. Создание буклета «Техника безопасности при работе с компьютером».

Тема № 3. (5 часов)
Проблемы Интернет-зависимости

1. Основные вопросы: ЗОЖ и компьютер. Деструктивная информация в Интернете - как ее избежать. Психологическое воздействие информации на человека. Управление личностью через сеть. Интернет и компьютерная зависимость (аддикция). Критерии зависимости с точки зрения психологов (приоритетность, изменения настроения, толерантность, симптом разрыва, конфликт, рецидив). Как развивается зависимость. Типы интернет - зависимости (пристрастие к работе с компьютером, к навигации и поиску информации, игромания и электронные покупки, зависимость от сетевого общения, сексуальные зависимости).

2. Требования к знаниям и умениям: Обучающиеся должны знать, что такое ЗОЖ, и как влияет компьютер на 13 здоровье, какое психологическое воздействие оказывает информация на личность человека, критерии зависимости, типы интернет-зависимости, как развивается зависимость. Обучающиеся должны уметь распознавать и избегать деструктивную информацию в Интернете, уметь вовремя выявить интернет-зависимость и сообщить специалистам.

3. Тематика практических работ: Практическая работа. «Создание мультимедийной презентации «ПК и ЗОЖ. Организация рабочего места».

Тема № 4. (6 часов)
Методы обеспечения безопасности ПК и Интернета.
Вирусы и антивирусы

1. Основные вопросы: Вирусы человека и компьютера, цели компьютерных вирусов. Типы вирусов. Отличия вирусов и закладок. Как распространяются вирусы. Что такое антивирусная защита. Как лечить компьютер. Антивирусные программы для ПК: сканеры, ревизоры и др. Выявление неизвестных вирусов. Защита мобильных устройств. Безопасность при скачивании файлов. Защита программ и данных от несанкционированного копирования. Организационные, юридические, программные и программно-аппаратные меры защиты. Защита программ и данных с помощью паролей, программных и электронных ключей, серийных номеров, переноса в онлайн и т.п. Методы защиты фото и видеоматериалов от копирования в сети. Проверка подлинности (аутентификация) в Интернете. Меры личной безопасности при сетевом общении. Настройки приватности в социальных сетях. Предотвращение несанкционированного

доступа к ПК. Пароли, биометрические методы защиты и аутентификация с помощью внешних носителей.
2. Требования к знаниям и умениям: Обучающиеся должны знать типы вирусов, что такое антивирусная защита, антивирусные программы, как лечить компьютер, как защитить мобильные устройства, как защитить фото и видеоматериалов от скачиваний. Обучающиеся должны уметь распознавать вирусы, пользоваться антивирусными защитными программами, соблюдать меры личной безопасности при сетевом общении.
3. Тематика практических работ: Практическая работа №1. «Установка антивирусной программы»; Практическая работа №2. Создание презентации на тему: «Разновидности вирусов. Черви, трояны, скрипты», «Шпионские программы». «Шифровальщики». «Троян-вымогатель в социальной сети "ВКонтакте" или наказание для особо любопытных».

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

1. 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.
2. 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.
3. Тематика практических работ: Практическая работа. Доклад на тему: «Правила поведения в сети с мошенниками и злоумышленниками», или «Как не стать жертвой сетевых шуток и розыгрышей».

Тема № 6. (5 часов)
Сетевой этикет. Психология и сеть

1. Основные вопросы: Что такое этикет. Виды этикета (личный, деловой, письменный, дискуссионный и пр.). Различия этикета в разных странах. Как появился этикет, что это такое. Сетевой этикет. Общие правила сетевого этикета. Этика дискуссий. Взаимное уважение при интернет-общении. Этикет и безопасность. Эмоции в сети, их выражение. Примеры этических нарушений. Безопасная работа в сети в процессе сетевой коммуникации (чаты, форумы, конференции, скайп, социальные сети и пр.). Термины сетевого этикета: оверквотинг, флейм, флуд, оффтопик, смайлики и др. Психологическая

обстановка в Интернете: грифинг, кибербуллинг, кибер-моббинг, троллинг, буллицид. Если вы стали жертвой компьютерной агрессии: службы помощи личное общение и общение в группе - чем они отличаются (чаты, форумы, службы мгновенных сообщений).
2. Требования к знаниям и умениям: 15 Обучающиеся должны знать сетевой этикет, этические и правовые нормы информационной деятельности человека, информационный этикет и право, информационную безопасность. Обучающиеся должны уметь использовать этические и правовые нормы информационной деятельности человека, информационный этикет и право, информационную безопасность.
3. Тематика практических работ: Практическая работа. «Выпуск видеоролика на тему «Как не испортить себе настроение при общении в Сети и не опуститься до уровня «веб-агрессора».

Тема №7. (5 часов)
Государственная политика в области кибербезопасности

1. Основные вопросы: Собственность в Интернете. Авторское право. Интеллектуальная собственность. Платная и бесплатная информация. Защита прав потребителей при использовании услуг Интернет. Защита прав потребителей услуг провайдера. Как расследуются преступления в сети. Ответственность за интернетмошенничество. Правовые акты в области информационных технологий и защиты киберпространства. Доктрина информационной безопасности.
2. Требования к знаниям и умениям: Обучающиеся должны знать правовые основы защиты от информации, причиняющей вред здоровью и развитию, интеллектуальной собственности, уголовной ответственности за создание, использование и распространение вредоносных компьютерных программ, авторского право, охраны программ для ЭВМ и баз данных(БД), лицензионных программ. Обучающиеся должны уметь пользоваться правовыми основами защиты от информации, причиняющей вред здоровью и развитию, интеллектуальной собственности, уголовной ответственности за создание, использование и распространение вредоносных компьютерных программ, авторским правом, охраны программ для ЭВМ и баз данных(БД), лицензионных программ.

МЕТОДИЧЕСКОЕ ОБЕСПЕЧЕНИЕ

В ходе реализации программы возможно использование различных методов и приёмов организации занятий: • по источнику получения информации - практический (опыты, упражнения); наглядный (иллюстрация, демонстрация, наблюдения обучающихся); словесный (объяснение, разъяснение, рассказ, беседа, инструктаж, лекция, дискуссия, диспут); работа с книгой (чтение, изучение, реферирование, цитирование, беглый просмотр, конспектирование); идеометод (просмотр, обучение, упражнение, контроль); • по характеру дидактической цели - приобретение знаний; формирование умений и навыков; применение знаний; формирование творческой деятельности; закрепление и контроль знаний, умений, навыков; • по характеру познавательной деятельности - поисковые; объяснительно-иллюстративные; репродуктивные; проблемного изложения; эвристические (частично-поисковые); исследовательские; • по соответствию

методов обучения логике общественно-исторического познания - организация наблюдения, накопление эмпирического материала; обобщение теоретической обработки фактических данных; практическая проверка правильности выводов и обобщений, выявление истины, соответствия содержания и формы, явления и сущности; • по соответствию методов обучения специфике изучаемого материала и форм мышления - научного познания реальной действительности; освоения искусства; практического применения знаний. Все эти методы и приёмы направлены на стимулирование познавательного интереса обучающихся и формирование творческих учений и навыков. При проектировании занятий необходимо придерживаться следующих принципов системно-деятельностного подхода: 22 принцип активной включенности школьников в освоение предлагаемой информации; принцип деятельности; принцип доступности; принцип системности; принцип рефлексивности; принцип мотивации; принцип открытости содержания образования. Принцип активной включенности обучающихся в освоение предлагаемой информации предполагает субъектную позицию школьника в образовательном процессе, обращение педагога к личностному опыту учащегося и обогащение его в процессе деятельности на занятии. Важной составляющей в этом случае является создание для школьников условий транслирования информации, полученной в ходе занятий, в принципы собственной жизнедеятельности. Введение деятельностных технологий в обучающий процесс предполагает учет следующих критериев: интерактивность; игровой, театрализованный контекст; совместную деятельность ребенка и взрослого; учет психолого-возрастных особенностей школьников; использование социокультурных технологий. Принцип доступности предполагает адекватность содержания и подачи предлагаемого материала применительно к возрастным и психологическим особенностям школьников, а также имеющемуся у них социальному опыту. Принцип системности позволяет целостно представить учащимся как положительные, так и отрицательные стороны использования сети интернет. Принцип рефлексивности предполагает организацию самостоятельной познавательной деятельности школьников на всех этапах занятий с целью вовлечения их в процесс осмысления полученной информации, соотнесения ее с имеющимся личным социальным опытом и включения приобретенного нового содержания и способов деятельности в собственную практику. Принцип мотивации. Проектировать занятие таким образом, чтобы мотивировать школьников на самостоятельный поиск новой информации относительно использования инфокоммуникационных технологий в познавательных и развивающих целях, стимулировать их творческие и познавательные мотивационные потребности. Использовать средства побуждающего и формирующего воздействия. Эти средства необходимо применять так, чтобы они способствовали развитию различных компонентов и сторон мотивации в их единстве. Поэтому они должны применяться в комплексе, включающем приемы побуждения: и за счет стимулирующего влияния содержания учебного материала, и за счет побуждающей функции методов обучения, и за счет сочетания различных видов деятельности. Все это в совокупности обеспечит 23 динамику развития положительных потребностно-мотивационных состояний учащихся в соответствии со структурой мотивационной основы деятельности. Принцип открытости содержания образования предполагает достаточно гибкое использование педагогом предложенной конструкции, не допуская при этом

искажения логики, содержательной точности и достоверности информации. Материально-техническое обеспечение реализации дополнительной общеобразовательной программы «Безопасность в сети Интернет» включает следующий перечень необходимого оборудования: 1. Компьютер; 2. Мультимедийный проектор. 3. Интерактивная доска 4. Доступ к сети Интернет.

СПИСОК ЛИТЕРАТУРЫ

Нормативные правовые акты:

1. Федеральный закон «О защите детей от информации, причиняющей вред их здоровью и развитию» от 29 декабря 2010 г. № 436-ФЗ - https: //rg.ru/2010/12/31 /deti-inform-dok.html;
2. Федеральный закон Российской Федерации от 21 июля 2011 г. №2 252-ФЗ «О внесении изменений в отдельные законодательные акты Российской Федерации в связи с принятием Федерального закона «О защите детей от информации, причиняющей вред их здоровью и развитию»
3. Федеральный закон от 29.12.2012 г. № 273-ФЗ «Об образовании в Российской Федерации» (с изм., внесенными Федеральными законами от 04.06.2014 г. № 145-ФЗ, от 06.04.2015 г. № 68-ФЗ)
4. Приказ Министерства образования и науки Российской Федерации от 30.08.2013 г. № 1015 (в ред. Приказов Минобрнауки России от 13.12.2013 г. №1342, от 28.05.2014 г. № 598, от 17.07.2015 г. № 734) «Об утверждении Порядка организации и осуществления образовательной деятельности по основным общеобразовательным программам - образовательным программам начального общего, основного общего и среднего общего образования
5. Приказ Минобрнауки России от 15 июня 2016 г. № 715 «Об утверждении Концепции развития школьных информационно-библиотечных центров
6. Постановление Главного государственного санитарного врача Российской Федерации от 29.12.2010 № 189 (ред. от 25.12.2013 г.) «Об утверждении СанПиН 2.4.2.2821-10 «Санитарно-эпидемиологические требования к условиям и организации обучения в общеобразовательных учреждениях».

Основная литература:

1. Бирюков А.А. Информационная безопасность защита и нападение 2 е издание: Издательство: ДМК-Пресс., 2017, 434 с.
2. Бирюков А.А. Информационная безопасность защита и нападение.: Издательство: ДМК-Пресс., 2012, 474 с.
3. Колесниченко Денис. Анонимность и безопасность в интернете. От чайника к пользователю. Самоучитель Издательство: БХВ-Петербург, 2012, 240с. 45
4. Мазаник Сергей. Безопасность компьютера. Защита от сбоев, вирусов и неисправностей: издательство: ЭКСМО, 2014, 256 с.
5. Мэйволд Э. Безопасность сетей (2-е изд.) Книги» Сетевые Технологии. Название: Безопасностьсетей: Издательство: М.: НОУ "Интуит", 2016,571 с.
6. Проскурин В.Г Защита в операционных системах: Издательство: Горячая линия-Телеком, 2014, 192 с.

Приложение

Тест по безопасности в сети Интернет
«Основы безопасности в Интернете» Осторожно, вирус!

1. Что является основным каналом распространения компьютерных вирусов?
a. Веб-страницы
b. Электронная почта
c. Флеш-накопители (флешки)

2. Для предотвращения заражения компьютера вирусами следует:
a. Не пользоваться Интернетом
b. Устанавливать и обновлять антивирусные средства
c. Не чихать и не кашлять рядом с компьютером

3. Если вирус обнаружен, следует:
a. Удалить его и предотвратить дальнейшее заражение
b. Установить какую разновидность имеет вирус
c. Выяснить как он попал на компьютер

4. Что не дает хакерам проникать в компьютер и просматривать файлы и документы:
a. Применение брандмауэра
b. Обновления операционной системы
c. Антивирусная программа

5. Какое незаконное действие преследуется в России согласно Уголовному Кодексу РФ?
a. Уничтожение компьютерных вирусов
b. Создание и распространение компьютерных вирусов и вредоносных программ
c. Установка программного обеспечения для защиты компьютера

6. Какую информацию нельзя разглашать в Интернете?
a. Свои увлечения
b. Свой псевдоним
c. Домашний адрес

7. Чем опасны социальные сети?
a. Личная информация может быть использована кем угодно в разных целях
b. При просмотре неопознанных ссылок компьютер может быть взломан
c. Все вышеперечисленное верно

8. Виртуальный собеседник предлагает встретиться, как следует поступить?
a. Посоветоваться с родителями и ничего не предпринимать без их согласия
b. Пойти на встречу одному
c. Пригласить с собой друга

9. Что в Интернете запрещено законом?
a. Размещать информацию о себе
b. Размещать информацию других без их согласия
c. Копировать файлы для личного использования

10. Действуют ли правила этикета в Интернете?
a. Интернет - пространство свободное от правил
b. В особых случаях
c. Да, как и в реальной жизни