

Муниципальное бюджетное общеобразовательное учреждение
«Оглухинская средняя общеобразовательная школа»
Крутинского муниципального района Омской области
ЦОЦ и ГП «Точка роста»

РАССМОТРЕНО И ПРИНЯТО

на методическом совете

МБОУ «Оглухинская сош»

Протокол № 1 от 28.08.2020

Председатель 



Дополнительная общеобразовательная
(общеразвивающая) программа
«Безопасность в сети Интернет»

Направленность: техническая

Целевая группа: 9-11 лет

Общая трудоемкость: 35 часов

Форма реализации: очная

Уровень сложности содержания программы: стартовый

Автор-составитель:
Румянцева Нина Николаевна,
педагог дополнительного образования

Пояснительная записка

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 «Безопасность в сети Интернет» разработана в связи с возросшей потребностью обеспечения информационной безопасности детей и подростков при организации урочной, внеурочной, факультативной деятельности.

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

Задачи обучения:

1. Способствовать формированию знаний о безопасном поведении при работе с информацией в сети Интернет;
2. Формировать умения соблюдать нормы информационной этики;
3. Формировать умения безопасной работы с информацией, анализировать и обобщать полученную информацию
4. Развивать компьютерную грамотность и информационную культуру личности в использовании информационных и коммуникационных технологий;
5. Развивать умение анализировать и систематизировать имеющуюся информацию;
6. Развивать познавательную и творческую активность в безопасном использовании информационных и коммуникационных технологий;

Содержание программного материала этих тем, как в теории, так и на практических занятиях составлена с учетом 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.

Объем программы

На весь период обучения для освоения программы запланировано 35 учебных часа.

Режим занятий

Занятия проводятся один раз в неделю по 1 часа. Наполняемость групп до 10 человек.

Планируемые результаты

Личностные:

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

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.

Предметные:

1. Сформированы знания о безопасном поведении при работе с компьютерными программами, в соцсетях и с информацией в сети Интернет;

2. Сформированы умения соблюдать нормы информационной и сетевой этики;
3. Сформированы умения безопасно работать с информацией, анализировать и обобщать полученную информацию.

Формы проведения занятий:

Формы организации деятельности: групповая, индивидуальная, индивидуально-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; квесты; создание буклетов и мультимедийных презентаций.

Учебно-тематическое планирование

№ п/п	Тема	Всего часов	Теоретические занятия	Практические занятия
1.	Техника безопасности. Общие сведения о безопасности ПК и Интернета	3	2	1
2.	Техника безопасности и экология	2	2	0
3.	Проблемы Интернет - зависимости	3	2	1
4.	Методы обеспечения безопасности ПК и Интернета. Вирусы и антивирусы.	3	1	1
5.	Мошеннические	3	2	1

	действия в Интернете. Киберпреступления			
6.	Сетевой этикет. Психология и сеть	2	1	1
7.	Государственная политика в области кибербезопасности	2	1	1
	Итого: 35 ч	18	11	6

СОДЕРЖАНИЕ ПРОГРАММЫ

Тема № 1. (3 часа) Техника безопасности. Общие сведения о безопасности ПК и Интернета.

1. Основные вопросы: Правила поведения в компьютерном классе.

Техника безопасности при работе с компьютером. Как устроены компьютер и интернет. Как работают мобильные устройства. Угрозы для мобильных устройств. Защита персональных данных, почему она нужна. Безопасный профиль в социальных сетях. Защита киберпространства как комплекс мероприятий, направленных на обеспечение информационной безопасности. Компьютерная и информационная безопасность, средства защиты от несанкционированного доступа к данным. Основные угрозы безопасности информации: утечки, потеря целостности, нарушение работоспособности системы, незаконное тиражирование (воспроизведение). Безопасные ресурсы для поиска.

2. Требования к знаниям и умениям: Обучающиеся должны знать как устроены компьютер и интернет, как работают мобильные устройства, какие существуют угрозы для мобильных устройств, что такое защита персональных данных, аспекты кибербезопасности, что такое компьютерная и информационная безопасность, что такое кибертерроризм и кибервойны, основные угрозы безопасности информации. Обучающиеся должны уметь

защищать свои персональные данные, своевременно обнаружить проблемы сети.

3. Тематика практических работ: 1. Практическая работа: **Конкурс** на тему: Составь информационный буклет «Моя безопасная сеть» или сделай групповую газету «Безопасность в Интернет». Лучшие работы будут презентованы на родительских собраниях.

Тема № 2. (2 часа) Техника безопасности и экология

1. Основные вопросы: 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.

Тема № 3. (3 часа) Проблемы Интернет-зависимости

1. Основные вопросы: ЗОЖ и компьютер. Психологическое воздействие информации на человека. Управление личностью через сеть. Интернет и компьютерная зависимость. Как развивается зависимость? Типы интернет - зависимости (пристрастие к работе с компьютером, к поиску информации, игромания и электронные покупки, зависимость от сетевого общения).

2. Требования к знаниям и умениям: Обучающиеся должны знать, что такое ЗОЖ, и как влияет компьютер на 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 родителям или педагогам.

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

Тема № 4. (3 часа) 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. Защита мобильных устройств. Безопасность при скачивании файлов. Защита программ и данных с помощью паролей. Меры личной безопасности при сетевом общении. Настройки приватности в социальных сетях. Предотвращение несанкционированного доступа к ПК. Пароли.

2. Требования к знаниям и умениям: Обучающиеся должны знать типы вирусов, что такое антивирусная защита, антивирусные программы, как лечить компьютер, как защитить мобильные устройства. Обучающиеся должны уметь пользоваться антивирусными защитными программами, соблюдать меры личной безопасности при сетевом общении.

3. Тематика практических работ: Практическая работа: Создание буктрейлера на тему: «Разновидности вирусов». «Троян-вымогатель в социальной сети “В Контакте” или наказание для особо любопытных».

Тема № 5. (3 часа) Мошеннические действия в Интернете. Киберпреступления.

1. Основные вопросы: Виды интернет - мошенничества (письма, реклама, охота за личными данными и т.п.). Мошеннические действия в сети. Ложные

антивирусы. Сбор «пожертвований» на благотворительность. Опасности мобильной связи. Предложения по установке вредоносных приложений. Мошеннические СМС. Прослушивание разговоров. Определение местоположения телефона. Азартные игры. Онлайн - казино. 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, понятия компьютерное пиратство, кибернаемники и кибердетективы. Обучающиеся должны уметь обезопасить себя при интернет-общении.

3. Тематика практических работ: Практическая работа. Проект на тему: «Правила поведения в сети».

Тема № 6. (2 часа) 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: гриффинг, 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: 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. Конкурс: Выпуск видеоролика на тему «Как не испортить себе настроение при общении в сети»? Работа победителя будет презентована на родительском собрании

Тема №7. (2 часа) Государственная политика в области кибербезопасности.

1. Основные вопросы: Интеллектуальная собственность. Платная и бесплатная информация. Защита прав потребителей при использовании услуг Интернет. Ответственность за интернет-мошенничество. Правовые акты в области информационных технологий и защиты киберпространства.

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 права, 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.

3. Тематика практических работ: Практическая работа: Конкурс «Буклет Правовые основы для защиты от спама или как защитить себя при общении в социальных сетях». Работа победителя будет показана всем ученикам лицея на классном часе.

Контрольно-оценочные средства

После прохождения крупных разделов программы, обучающиеся выполняют творческие работы. Оценка работ производится, как правило, в форме их коллективного просмотра с обсуждением их особенностей и достоинств.

Основной формой подведения итогов обучения по дополнительной общеобразовательной программе является аттестация.

В конце каждого года обучения выполняются зачётные проверочные работы, состоящие из теоретической и практической частей. По завершении программы обучения воспитанники сдают итоговый зачёт, включающий проверочную работу и защиту творческих авторских работ в области информационных технологий.

Условия реализации программы

Санитарно-гигиенические требования

Занятия проходят в кабинете, соответствующем требованиям техники безопасности, противопожарной безопасности, санитарным нормам. Кабинет хорошо освещаться и периодически проветриваться. Наличие аптечки с медикаментами для оказания первой медицинской помощи имеется.

Основная литература:

1. Бирюкова А.А. Информационная безопасность защита и нападение 2-е издание: Издательство ДМК –Пресс., 2017,434с.
2. Методическое пособие для работников системы общего образования Солдатов Г., Зотова Е., Лебашева М., Шляпников В., «Интернет: возможности ,компетенции, безопасность»,

Полезные ссылки для учителя:

- 1)<http://www.kaspersky.ru>-антивирус тему «Лаборатория Касперского»;
- 2)<http://www.onlandia.org.ua/rus/>- безопасная web –зона;
- 3)<http://www.interneshka.net>-международный онлайн-конкурс по безопасному использованию Интернета;

4) Рыжков В.Н. –Методика преподавания информатики//http://nto.immpu.sgu.ru/sites/default/files/3/___12697.pdf;

5)<http://www.saferinternet.ru-Портал> Российского Оргкомитета по безопасному использованию Интернета;

6)<http://content-filtering.ru-Интернет> СМИ «Ваш личный Интернет»;

7)<http://www.rgdb.ru-> Российская государственная детская библиотека

8)<http://www.saferinternet.ru/-Безопасный> Интернет. Портал Российского Оргкомитета по проведению Года Безопасного Интернета. Мероприятия ,Интернет и законодательство,проблемы и решения ,международнык ресурсы;

9)<http://www.saferinternet.ru/-> Центр Безопасного Интернета в России. Сайт посвящен проблеме безопасной ,корректной и комфортной работы в Интернете. Интернет-угрозы и эффективное противодействие им в отношении пользователей;

10)<http://www.fid.su/-Фонд> развития Интернета. Информация о проектах, конкурсах, конференциях и др. по компьютерной безопасности и безопасности Интернета;

11)<http://www.microsoft.com/Rus/athome/security/kids/etusivu/html> - Безопасность в Интернете. “Основы безопасности детей и молодежи в 30 Интернете”-интерактивный курс по Интернет-безопасности, предлагаемый российским офисом Microsoft в рамках глобальных инициатив Microsoft “Безопасность детей в Интернете” и “Партнерство в образовании”. В разделе для учащихся (7-16лет) предлагается изучить проблемы информационной безопасности посредством рассказов в картинках. В разделе для родителей и учителей содержится обновленная информация о том, как сделать Интернет для детей более безопасным, а так же изложены проблемы компьютерной безопасности.

Полезные ссылки для обучающихся:

1) http://www.symantec.ru/norton/clubsymantec/library/article.isp?aid=cs_teach_kids-ClubSymantec – единый источник сведений о безопасности в

Интернете. Статья для родителей «Расскажите детям о безопасности в Интернете». Информация о средствах родительского контроля ;

2) <http://obzh.info/novosti/novoe/bezopasnost-detei-v-internete.html> –
Личная безопасность. Основы безопасности жизни. Рекомендации взрослым: как сделать посещение Интернета для детей полностью безопасным;

3) <http://www.ifap.ru/library/book099.pdf> – «Безопасность детей в Интернете», компания Microsoft. Информация для родителей: памятки, советы, рекомендации;

4) <http://www.interneshka.net/children/index.phtml> – «Интернешка» – детский онлайн-конкурс по безопасному использованию сети Интернет. Советы детям, педагогам и родителям, «полезные ссылки». Регистрация и участие в конкурсе по безопасному использованию сети Интернет.