Муниципальное общеобразовательное учреждение
Барановская средняя общеобразовательная школа
Буйского муниципального района
Костромской области

РЕКОМЕНДОВАНА	«СОГЛАСОВАНО»	«УТВЕРЖДЕНО»
к утверждению педагогическим советом школы. Протокол № 1 От 31.08.2022 г.	Заместитель директора по УР МОУ Барановская СОШ _____ Е.С.Чайкина От 31.08.2022 г.	Директор МОУ Барановская СОШ _____ М.Н.Голубева Приказ № 56-1 от 31.08.2022 г.

РАБОЧАЯ ПРОГРАММА
ВНЕУРОЧНОЙ ДЕЯТЕЛЬНОСТИ
«Медиабезопасность»

Направление: Социальное
Курс обучения: 9 класс

Срок реализации программы:
2022-2023 учебный год

Автор: Голунова И.Н.
учитель информатики

Бараново, 2020

Оглавление

1.РЕЗУЛЬТАТЫ ОСВОЕНИЯ КУРСА ВНЕУРОЧНОЙ ДЕЯТЕЛЬНОСТИ..... 4

2.СОДЕРЖАНИЕ КУРСА ВНЕУРОЧНОЙ ДЕЯТЕЛЬНОСТИ,..... 5

ФОРМЫ ОРГАНИЗАЦИИ И ВИДЫ ДЕЯТЕЛЬНОСТИ..... 5

3.ТЕМАТИЧЕСКОЕ ПЛАНИРОВАНИЕ 8

Исследование проблемы медиабезопасности детей и подростков в последние годы является особенно актуальным в связи с бурным развитием IT-технологий и информационно-коммуникативных сетей. В настоящий момент увеличивается количество детей и подростков, использующих для общения сеть Интернет, играющих в компьютерные игры, проводящих значительную часть времени за просмотром мультсериалов и телевизионных шоу, что негативно влияет на социально – психологическое здоровье современных школьников.

Поэтому данная программа нацелена на решение следующих проблем:

- просвещение школьников по вопросам безопасного поведения в современном информационно-коммуникативном пространстве;

- формирование у учащихся навыков безопасного пользования информационно-коммуникативными сетями и интернетом, а также профилактика негативного влияния современных информационных технологий на психику современных школьников.

Цели обучения: формирование у учащихся навыков безопасного поведения в медиа пространстве и профилактика негативного влияния современных IT-технологий на психику школьников.

Задачи обучения:

- познакомить школьников с нормативно-правовыми документами по вопросам защиты детей от информации, причиняющей вред их здоровью и развитию;
- сформировать знания в области медиа безопасности детей, использующих Интернет, СМИ, различные виды телекоммуникаций;
- ознакомить с технологиями и средствами защиты информации;
- сформировать у учащихся навыки по профилактике и коррекции зависимого поведения, связанного с компьютерными технологиями и Интернетом.

Образовательная программа «Медиабезопасность подростков» разработана в связи с возросшей потребностью обеспечения информационной безопасности детей и подростков при обучении, организации внеучебной деятельности и свободном использовании современных информационно-коммуникационных технологий (Интернет, сотовая (мобильная) связь и СМИ). Медиабезопасность ребенка – это задача и семейного и школьного воспитания.

Программа разработана с учетом требований законов РФ: «Об образовании», «О защите детей от информации, причиняющей вред их здоровью и развитию» и «Санитарно-эпидемиологических требований к условиям и организации обучения в общеобразовательных учреждениях» СанПин 2.4.2.2821-10.

Особенности содержания программы:

Программа разработана на блочно-модульной основе и представляет совокупность отдельных модулей.

Сроки реализации программы: 2022-2023 учебный год.

1.РЕЗУЛЬТАТЫ ОСВОЕНИЯ КУРСА ВНЕУРОЧНОЙ ДЕЯТЕЛЬНОСТИ

Личностные результаты:

- наличие представлений об информации как важнейшем стратегическом ресурсе развития личности, государства, общества;
- понимание роли информационных процессов в современном мире;
- владение первичными навыками анализа и критичной оценки получаемой информации;
- ответственное отношение к информации с учетом правовых и этических аспектов ее распространения;
- развитие чувства личной ответственности за качество окружающей информационной среды;
- способность и готовность к общению и сотрудничеству со сверстниками и взрослыми в процессе образовательной, общественно-полезной, учебно-исследовательской, творческой деятельности;
- способность и готовность к принятию ценностей здорового образа жизни за счет знания основных гигиенических, эргономических и технических условий безопасной эксплуатации средств ИКТ.

Метапредметные результаты:

- владение умениями самостоятельно планировать пути достижения целей; соотносить свои действия с планируемыми результатами, осуществлять контроль своей деятельности, определять способы действий в рамках предложенных условий, корректировать свои действия в соответствии с изменяющейся ситуацией; оценивать правильность выполнения учебной задачи;
- владение основными универсальными умениями информационного характера: постановка и формулирование проблемы; поиск и выделение необходимой информации, применение методов информационного поиска; структурирование и визуализация информации; выбор наиболее эффективных способов решения задач в зависимости от конкретных условий; самостоятельное создание алгоритмов деятельности при решении проблем творческого и поискового характера;
- ИКТ-компетентность – широкий спектр умений и навыков использования средств информационных и коммуникационных технологий для сбора, хранения, преобразования и передачи различных видов информации, навыки создания личного информационного пространства.

Предметные результаты:

- формирование информационной и алгоритмической культуры; формирование представления о компьютере как универсальном устройстве обработки информации; развитие основных навыков и умений использования компьютерных устройств;
- формирование представления об основных изучаемых понятиях: информация, алгоритм, модель – и их свойствах;
- развитие алгоритмического мышления, необходимого для профессиональной деятельности в современном обществе; развитие умений составить и записать алгоритм для конкретного исполнителя; формирование знаний об алгоритмических конструкциях,

логических значениях и операциях; знакомство с одним из языков программирования и основными алгоритмическими структурами — линейной, условной и циклической;

● формирование умений формализации и структурирования информации, умения выбирать способ представления данных в соответствии с поставленной задачей — таблицы, схемы, графики, диаграммы, с использованием соответствующих программных средств обработки данных;

● формирование навыков и умений безопасного и целесообразного поведения при работе с компьютерными программами и в Интернете, умения соблюдать нормы информационной этики и права.

2.СОДЕРЖАНИЕ КУРСА ВНЕУРОЧНОЙ ДЕЯТЕЛЬНОСТИ, ФОРМЫ ОРГАНИЗАЦИИ И ВИДЫ ДЕЯТЕЛЬНОСТИ

МОДУЛЬ 1. СОХРАНЕНИЕ ФИЗИЧЕСКОГО И ПСИХИЧЕСКОГО ЗДОРОВЬЯ ДЕТЕЙ ПРИ РАБОТЕ С КОМПЬЮТЕРОМ

Тема 1.1 **Здоровьесберегающие технологии при работе на ПК в общеобразовательных учреждениях**

Здоровьесберегающие технологии, применяемые при организации работы школьника на компьютере. Профилактика нарушений здоровья детей в современной информационной среде.

Тема 1.2 **Гигиенические требования к организации занятий с использованием ИКТ**

Гигиенические требования к организации занятий с использованием новых информационно-компьютерных технологий.

Тема 1.3 **Негативное воздействие компьютера на психическое здоровье детей**

Воздействие компьютера на психическое здоровье детей. Уход от реальности. Признаки, характерные для игромании, как разновидности зависимого поведения. Стресс при работе с компьютером. Способы его профилактики и коррекции.

МОДУЛЬ 2. ИНФОРМАЦИОННАЯ ЭТИКА И ПРАВОВЫЕ АСПЕКТЫ ЗАЩИТЫ ИНФОРМАЦИИ

Тема 2.1 **Этика и право при создании и использовании информации**

Сетевой этикет. Информационная безопасность. Угрозы информационной безопасности. Уровни информационной безопасности. Направления защиты компьютерной информации.

Тема 2.2 **Основные законы Российской Федерации в области компьютерного права**

Федеральный закон «О защите детей от информации, причиняющей вред их здоровью и развитию» (от 29.12.2010 г. № 436-ФЗ –1 с последующим изменением и дополнением) Федеральный закон «О введении в действие части четвертой Гражданского кодекса РФ» (от

18.12.2006 г. № 231-ФЗ).

Федеральный закон «О связи» (от 07.07.2003 г. № 126-ФЗ с последующим изменением и дополнением). Федеральный закон «Об информации, информационных технологиях и защите информации» (от 27.07.2006 г. № 149-ФЗ).

МОДУЛЬ 3. ЗАЩИТА ДЕТЕЙ И ПОДРОСТКОВ ОТ НЕГАТИВНОГО ВЛИЯНИЯ СОВРЕМЕННЫХ ТЕЛЕКОММУНИКАЦИЙ

Тема 3.1 Опасность, подстерегающая в сети Интернет

Риск получения ребенком доступа к информации, причиняющей вред эмоциональному и психическому здоровью детей и подростков. Основные угрозы безопасности детей в Интернете: заражение вредоносным ПО, неконтролируемые покупки, киберхулиганы, злоупотребление общим доступом к файлам, неприличный контент, вторжение в частную жизнь. Советы по безопасности при работе на общедоступном компьютере.

Тема 3.2 Организация безопасного поиска информации в сети Интернет

Организация правильного поиска необходимой информации в сети Интернет и СМИ. Формирование запросов в поисковых системах.

Тема 3.3 Безопасное общение детей в Интернете: социальные сети, чаты, электронная почта

Противостояние угрозам из Интернета. Инструкции по безопасному общению в чатах, социальных сетях, электронной почте. Интернет-этика поведения в Интернете. Безопасное общение при использовании мобильной (сотовой) связи.

Тема 3.4 Профилактика Интернет - зависимости

Профилактика Интернет - зависимости. Преодоление Интернет - зависимости у детей и подростков.

МОДУЛЬ 4. ТЕХНОЛОГИИ И СРЕДСТВА ЗАЩИТЫ ИНФОРМАЦИИ ОТ НЕСАНКЦИОНИРОВАННОГО ДОСТУПА

Тема 4.1 Способы защиты информации

Цели совершения преступления. Основные понятия в области защиты информации от разрушения и несанкционированного доступа. Уровни защиты информации. Меры по защите информации. Планирование мер по защите информации на создаваемые электронные ресурсы.

Тема 4.2 Меры безопасности при работе с электронной почтой

Основные угрозы личной безопасности: кража индентификационных сведений, мистификация, нежелательная почта (спам). Доступ к файловой системе (папкам). Утечка информации через электронную почту. Меры безопасности при работе с электронной почтой.

Тема 4.3. Основы безопасности при общении в социальных сетях

Основные угрозы: кража персональных сведений, фишинг, доступ к информации, хранящееся на компьютере, использование информации, опубликованной на личной страничке в корыстных целях и др. Меры предосторожности при общении в социальных сетях.

Тема 4.4 **Основы безопасности мобильной (сотовой) связи.**

Основы безопасности при использовании мобильной (сотовой) связи. Виды мошенничества в мобильной связи. Меры предосторожности и безопасности при использовании сотовой (мобильной) связи.

МОДУЛЬ 5. КОМПЬЮТЕРНЫЕ ВИРУСЫ И СРЕДСТВА ЗАЩИТЫ

Тема 5.1. **Виды компьютерных вирусов**

Обзор и классификация компьютерных вирусов. Способы распространения вирусов. История вредоносных программ. Вирусная терминология. Классификация вирусов. Самые распространенные вирусы. Цикл функционирования вирусов.

Тема 5.2. **Антивирусные программы и файрволы**

Антивирусное программное обеспечение и антишпионские программы, межсетевые экраны. Методы борьбы с вирусами. Меры защиты от проникновения и распространения вирусов.

ФОРМЫ ПРОВЕДЕНИЯ ЗАНЯТИЙ

1.теоретическое занятие;

2.самостоятельная работа (ученики выполняют индивидуальные задания в течение части занятия или одного-двух занятий);

3.проектная деятельность (получение новых знаний, реализация личных проектов);

4.практическое занятие (ученикам предоставляется возможность познакомиться: с опасностями, подстерегающими в сети Интернет;

5.с организацией безопасного поиска информации в сети Интернет; со способами защиты информации; мерами безопасности при работе с электронной почтой; с основами безопасности мобильной связи и при общении в социальных сетях; с видами компьютерных вирусов и антивирусными программами)

ВИДЫ ДЕЯТЕЛЬНОСТИ УЧАЩИХСЯ

- индивидуальная и групповая конструкторская, техническая, научно-исследовательская работа;
- коллективные, парные и индивидуальные творческие, технические проекты;
- индивидуальные и групповые беседы;
- круглый стол, мозговой штурм;
- игровые программы, игры, конкурсы, участие в соревнованиях, конкурсах, фестивалях.

ТРЕБОВАНИЯ К РЕЗУЛЬТАТАМ ОБУЧЕНИЯ

Результатами освоения программы являются:

- осознание обучающимися значимости проблемы медиабезопасности;

- *сформированные* компетентности в области правовых аспектов медиабезопасности детей и подростков;
- знание способов защиты от противоправных посягательств в сети Интернет и мобильной (сотовой) связи.

3.ТЕМАТИЧЕСКОЕ ПЛАНИРОВАНИЕ

№ п/п	Наименование модулей и тем	Количество часов	Лекции	Практические занятия
1	МОДУЛЬ 1. Сохранение физического и психического здоровья детей при работе с компьютером	**8**	**6**	**2**
2	МОДУЛЬ 2. Информационная этика и правовые аспекты защиты информации	**4**	**4**	
3	МОДУЛЬ 3. Защита детей и подростков от негативного влияния современных телекоммуникаций	**9**	**3**	**6**
4	МОДУЛЬ 4. Технологии и средства защиты информации от несанкционированного доступа	**7**	**2**	**6**
5	МОДУЛЬ 5. Компьютерные вирусы и средства защиты	**6**	**2**	**4**
	Всего:	***34***	***17***	***18***

Приложение

ТЕМАТИЧЕСКИЙ ПЛАН КУРСА

(1 час в неделю)

№ п/п	Наименование модулей и тем	Количество часов	Дата	
			По плану	Фактически
МОДУЛЬ 1. Сохранение физического и психического здоровья детей при работе с компьютером (8 часов)				
1-4	Здоровье сберегающие технологии при работе на компьютере	**4**		
5-6	Гигиенические требования к организации занятий с использованием ИКТ	**2**		
7-8	Негативное воздействие компьютера на психическое здоровье детей	**2**		
МОДУЛЬ 2. Информационная этика и правовые аспекты защиты информации (4 часа)				
9-10	Этика и право при создании и использовании информации	**2**		
11-12	Основные законы Российской Федерации в области компьютерного права	**2**		
МОДУЛЬ 3. Защита детей и подростков от негативного влияния современных телекоммуникаций (9 часов)				
13-14	Опасность, подстерегающая в сети Интернет	**2**		
15-18	Организация безопасного поиска информации в сети Интернет	**4**		
19-20	Безопасное общение детей в Интернете: социальные сети, чаты, электронная почта	**2**		
21	Профилактика Интернет-зависимости	**1**		
МОДУЛЬ 4. Технологии и средства защиты информации от несанкционированного доступа (8 часов)				
22-23	Способы защиты информации	**2**		
24-25	Меры безопасности при работе с электронной почтой	**2**		
26-27	Основы безопасности при общении в социальных сетях	**2**		
28-29	Основы безопасности мобильной (сотовой) связи.	**2**		
МОДУЛЬ 5. Компьютерные вирусы и средства защиты (6 часов)				
30-32	Виды компьютерных вирусов	**3**		
33-34	Антивирусные программы и файрволы	**3**		
	Всего:	***34***		

СПИСОК РЕКОМЕНДУЕМОЙ ЛИТЕРАТУРЫ

1.Беки Уорли. Интернет: реальные и мнимые угрозы/ Пер. с англ. — М.: КУДИЦ- ОБРАЗ, 2004. — 320 с.

2.Галатенко В.А. Основы информационной безопасности. [Текст] 4-е изд. учеб. пособие, ВУЗ // — М: Издательство Бином. Лаборатория знаний, Интуит, 2008— 205 с.

3. Горбунова Л.Н., Анеликова Л.А., Семибратов А.М., Смирнов Н.К., Сорокина Е.В., Третьяк Т.М. Здоровье и безопасность детей в мире компьютерных технологий и Интернет. [Текст] Учебно-методический комплект. - М.: СОЛОНПРЕСС, 2010. - 176 с.: ил.

4. Федеральный закон «О защите детей от информации, причиняющей вред их здоровью и развитию» от 29 декабря 2010 года N 436-ФЗ;

5. Федеральный закон Российской Федерации от 21 июля 2011 г. N 252-ФЗ г. Москва «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»; 6.«Санитарно-эпидемиологических требований к условиям и организации обучения в общеобразовательных учреждениях» СанПин 2.4.2.2821-10.

6. «Школьный психолог», методическая газета для педагогов-психологов №12/2006, статья «Телевидение и нравственность: возможен ли союз?» И.Гундоровой;

7.«Школьный психолог», методическая газета для педагогов-психологов №19/2006, статья «Зависимость от компьютера» О. Решетниковой;

8.«Санитарно-эпидемиологических требований к условиям и организации обучения в общеобразовательных учреждениях» СанПин 2.4.2.2821-10.

9.Лаборатория Касперского (Электронный ресурс).-URL: http://www.kaspersky.ru/keeping_children_safe

10.Компьютерный информационный портал (электронный ресурс)

URL: http://www.oszone.net/6213/

11.Безопасность детей в Интернете. Nachalka.com 2008 [Электронный ресурс]. —

URL: http://www.nachalka.com/bezopasnost