Отдел образования администрации Первомайского района
Муниципальное бюджетное общеобразовательное учреждение
«Первомайская средняя общеобразовательная школа»
Первомайского района Тамбовской области
(филиал в с.Хобот-Богоявленское)

Рекомендована
к утверждению на заседании
методического совета
протокол № 4 от 26.04.2022 года

Утверждаю
Директор
МБОУ «Первомайская средняя
общеобразовательная школа»
_____Л.А.Груздева
приказ от29.04.2022 года №78/1

Дополнительная общеобразовательная общеразвивающая программа социально-педагогической направленности «Безопасность.RU»

для детей школьного возраста (11-16 лет)
Срок реализации – 21 час

Автор составитель
программы:
Грязнева Нина Ивановна,
учитель химии

с. Хобот-Богоявленское, 2022г.

ИНФОРМАЦИОННАЯ КАРТА ПРОГРАММЫ

1. Учреждение	Филиал муниципального бюджетного образовательного учреждения «Первомайская средняя общеобразовательная школа» в селе Хобот - Богоявленское Первомайского района Тамбовской области
2. Полное название программы	Дополнительная общеобразовательная общеразвивающая программа «Безопасность.RU»
3. Сведения об авторах:	
3.1. Ф.И.О., должность	***Грязнева Нина Ивановна*** – учитель химии
4. Сведения о программе:	
4.1. Нормативная база:	-Закон «Об образовании РФ» -Конвенция о правах ребенка, ООН, 1991г. -Положение об оздоровительном лагере. -Правила внутреннего распорядка лагеря. -Правила по технике безопасности, пожарной безопасности. -Рекомендации по профилактике детского травматизма, предупреждению несчастных случаев с детьми в оздоровительном лагере. -Инструкции по организации и проведению экскурсий. -Должностные инструкции работников. -Санитарные правила о прохождении медицинского осмотра. -Заявления от родителей. -Акт приемки лагеря. -Планы работы.
4.2. Область применения	Дополнительное образование
4.3. Направленность	Информационная
4.4. Тип программы	Модифицированная
4.5. Целевая направленность программы	Образовательная
4.6. Возраст учащихся по программе	11- 16 лет
4.7. Продолжительность обучения	21 час

Блок №1. «Комплекс основных характеристик дополнительной обшеобразовательной общеразвивающей программы «Безопасность.RU»

1.1.Пояснительная записка

Детские лагеря, несомненно, являются неотъемлемой частью системы дополнительного образования, которая обеспечивает детям возможности всестороннего удовлетворения его творческих потребностей в сфере досуга.

Лагерь - это форма активного отдыха, разнообразная социально значимая спортивно-оздоровительная и досуговая деятельность, отличающаяся от учебной деятельности. Он дает возможность каждому ребенку раскрыться, повысить уровень самоуважения и самореабилитации. Лагерь с дневным пребыванием учащихся призван создать благоприятные условия для полноценного отдыха детей.

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).

Актуальность программы обусловлена возрастающими объёмами цифровой информации в мире и, следовательно, необходимостью овладения компетенциями, связанными с безопасной деятельностью в информационной среде. В современных условиях Интернет является глобальным и обширным источником информации, создает условия для обучения и коммуникации, творческой реализации и проведения досуга. В то же время пространство цифровой коммуникации содержит множество опасностей при повседневном пользовании: кибермошенничество, буллинг, преступные действия в отношении кражи персональных данных и т.д.

Программа направлена на формирование у обучающихся навыков в сфере противостояния негативной информации, размещенной в сети Интернет, и соблюдения персональной безопасности в информационном

пространстве; практических умений по противостоянию угрозам здоровью и жизни несовершеннолетних, источником которых является вредоносная информация, содержащаяся в информационном поле.

Отличительные особенности Программы состоят в универсальности выбранного подхода и ее практической направленности. Реализация Программы не требует специальной базовой подготовки слушателей, а нацелена на формирование навыков безопасности в сети Интернет любого пользователя, а значит, обеспечивает принцип системности и взаимосвязи всех уровней образования, поскольку компетенции в сфере поиска, критического восприятия и обработки информации в интернет-пространстве являются актуальными как для общего образования, так и для последующих уровней образования. Программа опирается также на принцип построения здоровьесберегающего пространства, неотъемлемой частью которого в современном мире является безопасность человека в глобальном информационном мире.

При реализации Программы возможно привлечение педагогов-психологов при изучении таких актуальных тем для информационной безопасности, как кибербуллинг и профилактика интернет-зависимости

Возрастные особенности учащихся

Средний школьный возраст- переходный возраст от детства к юности, характеризующийся глубокой перестройкой организма.

Объем и срок освоения программы

21 час

Формы обучения - очная, допускается сочетание различных форм получения образования и форм обучения.

Цель дополнительной общеразвивающей программы состоит в формировании у слушателей базовых принципов безопасного поведения в информационном пространстве.

В соответствии с поставленной целью в Программе решаются следующие группы **задач**:

- *развивающие:* развивать информационную культуру личности; развивать навыки критического мышления и восприятия различной информации; развивать логическое мышление и познавательную активность;
- *образовательные*: сформировать знания о безопасном поведении в сети Интернет; нормах сетевого этикета; умения осуществлять поиск, критическое осмысление и анализ информации в сети Интернет;
- *воспитательные*: формировать ценностное отношение к личности в процессе коммуникации к персональной безопасности в сети Интернет; формировать сознательное отношение к вопросам личной безопасности как элемента здоровьесберегающей среды; продолжить формирование активной гражданской позиции;

Планируемые результаты. В результате освоения Программы слушатели будут *знать*:

– понятия «персональные данные», «информационное общество», «цифровой след»; «персональная безопасность в сети»;

– понятия фишинга и вредоносного программного обеспечения, безопасного серфинга в сети Интернет;

– правила безопасного использования онлайн-сервисов и интернет-ресурсов; защиты персональных данных в сети;

– правила сетевого этикета и общения в социальных сетях;

– способы защиты от кибермошенничества;

– основы безопасной работы с мобильными устройствами;

– правила здоровьесбережения при работе с персональными компьютерами и мобильными устройствами.

В результате освоения Программы слушатели будут *уметь*:

– осуществлять поиск и анализ необходимой информации;

– распознавать вредоносные сайты, угрожающие жизни и здоровью

подростков;

– применять полученные знания при использовании ресурсов сети Интернет на персональном компьютере и мобильном устройстве;

– высказывать свою позицию по вопросу личной безопасности в сети Интернет.

В результате освоения Программы слушатели буду *иметь навыки*:

– идентификации негативной информации, источником которой является Интернет, нейтрализации ее пагубного воздействия;

– графического оформления теоретического материала;

– оценивания своей работы и взаимооценивания;

– поиска и критического осмысления информации, полученной из интернет-источников.

1.2.Цель программы:

формирование у слушателей базовых принципов безопасного поведения в информационном пространстве

1.3. Содержание программы

Тема 1. Инструктаж по технике безопасности. Информация и интернет (1 час).

Теория: техника безопасности при работе с персональным компьютером; понятие «информации», роль информации для современного общества; классификация информации. Интернет как способ поиска информации. Правила осуществления поиска, анализа и обработки информации в сети Интернет. Браузеры и их роль в поиске информации.

Тема 2. Что такое информационное общество (1 час).

Теория: определение информационного общества, основные идеи; взаимосвязь информационного общества и цифровой экономики; роль информационных технологий в жизни современного общества; концепция информационного общества в России.

После изучения темы предусмотрен текущий контроль.

Тема 3. Понятие персональных данных. (2 час).

Теория: понятие персональных данных; функции персональных данных; состав персональных данных; использование персональных данных в сети Интернет: сервисы и услуги; важность защиты персональных данных; защита персональных данных и цифровые технологии.

После изучения темы предусмотрено тестирование.

Тема 4. Защита информации и кибербезопасность. Безопасный серфинг в Интернете (3 часов).

Теория: Что такое безопасный серфинг в Интернете? Понятие «кибербезопасности». Способы защиты персональных данных в Интернете: пароли, изучение политики конфиденциональности, разрешения для приложений, настройки браузера, временные файлы интернета, блокировка рекламы, защищенное соединение, резервное копирование важной информации, спам и т.д. Правила безопасного пользования электронной почтой. Законодательство в сфере информационной безопасности.

Тема 5. Безопасное общение в сети Интернет (3 часов).

Теория: Интернет как пространство коммуникации. Способы общения в сети Интернет: электронная почта, социальные сети, мессенджеры. Правила защиты от кибербуллинга. Недопустимость агрессивного участия в кибербуллинге. Понятие сетевого этикета. Правила общения в социальных сетях. Защита от негативной информации в социальных сетях. Овершеринг и его последствия. Цифровой след.

Тема 6. Безопасность в сети Wi-Fi. (2 часа).

Теория: что такое Wi-Fi и как его использовать. Главные опасности использования беспроводной сети. Правила безопасности при использовании Wi-Fi.

После изучения темы предусмотрен устный опрос.

Тема 7. Правила безопасного использования онлайн-сервисов и интернет-ресурсов. Потенциально опасные сайты (3часа).

Теория: способы различения потенциально-опасных сайтов. Предупреждение антивирусных программ о потенциальной опасности сайта и его нежелательном посещении. Фишинг.

Тема 8. Правила безопасного использования мобильных устройств (3 часа).

Теория: интернет и мобильные устройства. Мобильные приложения. Недопустимость использования программного обеспечения из недостоверных источников для мобильных устройств. Правила защиты мобильных устройств.

Тема 9. Защита от кибермошенничества (2 часа).

Теория: что такое кибермошенничество. Персональные данные и личные средства как объект кибермошенничества. Способы распознавания кибермошенников. Как не стать жертвой кибермошенников.

После изучения темы предусмотрено тестирование.

Тема 10. Интернет-зависимость и как ее избежать (1 час).

Теория: что такое интернет-зависимость. Интернет-зависимость как патология. Значение здорового образа жизни для профилактики интернет-зависимости. Расширение кругозора, увлечений, общения со сверстниками как профилактика интернет-зависимости. Признаки интернет-зависимости.

Учебный план

№	Название темы, раздела	Количество часов			Формы контроля
		всего	теория	практика	
1	Инструктаж по технике безопасности. Информация и Интернет	1	1	0	Устный опрос
2	Что такое информационное общество?	1	1	0	Текущий контроль. Опрос.
3	Понятие персональных данных	2	2	0	Тестирование, беседа
4	Защита информации и кибербезопасность. Безопасный серфинг в Интернете	3	2	1	Текущий контроль; практическое занятие
5	Безопасное общение в сети Интернет	3	2	1	Тестирование практическое занятие
6	Безопасность в сети Wi-Fi	2	2	0	Устный опрос
7	Правила безопасного использования онлайн-сервисов и интернет-ресурсов. Потенциально опасные сайты	3	2	1	Тестирование, беседа практическое занятие
8	Правила безопасного использования мобильных устройств	3	2	1	Тестирование, беседа
9	Защита от кибер-мошенничества	2	2	0	опрос
10	Интернет-зависимость: что это такое и как ее избежать	1	1	0	Опрос анкетирование
	ИТОГО	**21**	**17**	**4**	

Блок №2. «Комплекс организационно-педагогических условий»

Критерии эффективности программы

Для того чтобы программа была реализована, необходимо создать такие условия, чтобы каждый участник процесса (воспитатель и ребёнок) чувствовал себя комфортно в лагере, с удовольствием относился к обязанностям и поручениям, с радостью участвовал в предложенных мероприятиях. Для выполнения этих условий разработаны следующие критерии эффективности:

– постановка реальных целей и планирование результатов программы;

– заинтересованность педагогов и детей в реализации программы, благоприятный психологический климат;

– удовлетворённость детей и взрослых предложенными формами работы;

– творческое сотрудничество взрослых и детей.

Формы аттестации и оценочные материалы

Результативность освоения материала в рамках Программы отслеживается систематически с привлечение различных видов контроля:

– текущий контроль осуществляется на каждом занятии в форме различных видов опроса;

– наблюдение осуществляется в ходе выполнения слушателями практических работ;

– по результатам проверки различного вида заданий педагогом осуществляется не только оценка правильности выполнения, но и степени участия и активности обучающихся;

– для проверки знания ключевых понятий курса осуществляется тестирование;

– в ходе бесед и опросов слушатели формулируют и обосновывают свою позицию по отношению к вопросам персональной безопасности в сети

Интернет; педагогом также осуществляется проверка сформированности основ информационной культуры;

– итоговый контроль осуществляется в форме демонстрации слушателями результатов практической работы творческого характера по оформлению буклета, презентации, инфографки (на выбор) по вопросам изученного в рамках Программы материала.

Организационно-педагогические условия реализации программы

Материально-технические условия реализации Программы

Реализация Программы предполагает наличие компьютерного класса, оборудованного персональными компьютерами по количеству слушателей с лицензионным программным обеспечением и выходом в Интернет; мультимедийного мобильного комплекса.

Методическое обеспечение Программы.

Методическое обеспечение Программы включает лекционный, дидактический и наглядно-иллюстративный материал по вопросам безопасности в сети Интернет; тестовые задания, анкеты. Для проведения занятий привлекаются материалы, размещенные на специализированный ресурсах (Урок Цифры.рф, Единый урок.рф, Онлайн-школа «Фоксфорд», проект «Онлайн-уроки финансовой грамотности» и т.д,), включающие графическое представление основных положений личной безопасности в сети Интернет, видеофрагменты, квесты, тренажеры, онлайн-уроки и т.д. Предполагается, что предложенные интернет-ресурсы будут играть роль своеобразной памятки для слушателей по безопасному серфингу в Интернете. Опора на интернет-источники при проведении занятий обусловлена не только значимостью их информационного содержания, но и связана с формированием навыков пользования цифровыми ресурсами сети Интернет.

Основной формой проведения занятий является комбинированная, которая сочетает теоретический материал и выполнение самостоятельной работы.

Опрос осуществляется с элементами дискуссии, обсуждения основных вопросов безопасности в сети Интернет; в структуру занятия включаются проблемные ситуации по различным темам, которые предполагают либо выбор предложенного педагогом варианта решения и его аргументация, либо формулировка решения слушателями и его обоснование.

Литература

1. Внуков, А.А. Основы информационной безопасности: защита информации: учебное пособие для среднего профессионального образования / А. А. Внуков. - 3-е изд., перераб. и доп. - Москва: Издательство Юрайт, 2021. - 161 с. - (Профессиональное образование). - ISBN 978-5-534-13948-8. - Текст: электронный // ЭБС Юрайт [сайт]. - URL: https://urait.ru/bcode/475890

2. Казарин, О.В. Основы информационной безопасности: надежность и безопасность программного обеспечения: учебное пособие для среднего профессионального образования / О. В. Казарин, И. Б. Шубинский. - Москва: Издательство Юрайт, 2021. - 342 с. - (Профессиональное образование). - ISBN 978-5-534-10671-8. - Текст: электронный // ЭБС Юрайт [сайт]. - URL: https://urait.ru/bcode/475889

3. Методические рекомендации по реализации мер, направленных на обеспечение безопасности детей в сети «Интернет» (подготовлены членом Совета Федерации Федерального Собрания Российской Федерации Л.Н. Боковой) [Электронный ресурс] //Министерство цифрового развития, связи и массовых коммуникаций Российской Федерации: официальный сайт // Режим доступа: URL: https://digital.gov.ru/ru/documents/6406/

4. Методические рекомендации по основам информационной безопасности для обучающихся общеобразовательных организаций с учётом информационных, потребительских, технических и коммуникативных аспектов информационной безопасности [Электронный ресурс] // Единыйурок.рф: официальный сайт // Режим доступа: URL: https://единыйурок.рф/images/doc/metod/cyber.pdf

5. Научный, периодический, информационно-методический журнал с базовой специализацией в области информационной безопасности «Вопросы кибербезопасности» // Научная электронная библиотека «КиберЛенинка»:

официальный сайт // // Режим доступа: URL: https://cyberleninka.ru/journal/n/voprosy-kiberbezopasnosti?i=1072610

6. Письмо Минпросвещения России от 29.03.2019 №03-393 "О методических рекомендациях" (вместе с "методическими рекомендациями по реализации мер, направленных на обеспечение безопасности детей в сети "интернет") [Электронный ресурс] // ТОГБУ «Компьютерный центр»: официальный сайт // Режим доступа: URL: https://compcentr.68edu.ru/index.php/tsentr/index.php/tekhnicheskaya-podderzhka-5/skf/materialy/832-03-393

Интернет-ресурсы

1.Безопасность в Интернете - проект Городского методического центра [Электронный ресурс] // Mosmetod.ru: официальный сайт // Режим доступа: URL:http://security.mosmetod.ru/

2.Безопасность детей в сети Интернет [Электронный ресурс] // Подросток и общество: официальный сайт // Режим доступа: URL: https://podrostok.68edu.ru/?p=829

3.Безопасный Интернет - детям [Электронный ресурс] // Министерство внутренних дел Российской Федерации: официальный сайт // Режим доступа: URL:https://мвд.рф/mvd/structure1/Upravlenija/Upravlenie_K_MVD_Rossii/безопасный-интернет-детям

4.Единый урок по безопасности в сети Интернет: официальный сайт проекта [Электронный ресурс] // Режим доступа: URL: https://единыйурок.рф/index.php/plan-meropriyatij-kontseptsii-bezopasnosti/edinyj-urok-po-bezopasnosti-v-seti-internet-2018

5.Информационные ресурсы и сервисы Интернета. Поиск информации в сети Интернет [Электронный ресурс] // Российская электронная школа: официальный сайт // Режим доступа: URL: https://resh.edu.ru/subject/lesson/3051/train/#188223

6.Онлайн-урок «Как защититься от кибермошенничества. Правила безопасности в киберпространстве» [Электронный ресурс] // Онлайн-уроки по финансовой грамотности: официальный сайт // Режим доступа: URL: https://dni-fg.ru/kibersafe

7.Как обеспечить безопасность детей в Интернете [Электронный ресурс] // Онлайн-школа «Фоксфорд»: официальный сайт // Режим доступа: https://externat.foxford.ru/polezno-znat/bezopasnost-detej-v-internete

8.Кибербезопасность: как защитить личные данные в сети [Электронный ресурс] // Онлайн-школа «Фоксфорд»: официальный сайт // Режим доступа: URL:https://media.foxford.ru/kak-zashhitit-lichnye-dannye-v-seti/

9.Онлайн-урок «Как защититься от кибермошенников: семь правил безопасности в виртуальной среде» // Онлайн-уроки по финансовой грамотности: официальный сайт // Режим доступа: URL: https://dni-fg.ru/spec_kiber

10.Онлайн-урок «Твой безопасный банк в кармане» // Онлайн-уроки по финансовой грамотности: официальный сайт // Режим доступа: URL: https://dni-fg.ru/credit_cards

11.Приватность в цифровом мире: Урок Цифры [Электронный ресурс] // Урок Цифры.рф: официальный сайт // Режим доступа: URL: https://урокцифры.рф/lessons/cybersecurity

12.Общие рекомендации по обеспечению безопасности в сети Интернет [Электронный ресурс] // Министерство внутренних дел Российской

Федерации: официальный сайт // Режим доступа: URL:https://мвд.рф/вопросы/внимание-мошенники/безопасность-в-сети-интернет

13.Приключения робота Каспера. Овершеринг. Вред репутации [Электронный ресурс] // Лаборатория Касперского: официальный сайт // Режим доступа: URL: https://kids.kaspersky.ru/article/multfilm_priklyucheniya_robota_kaspera__overshering_vred_reputacii

14.Проект «Персональные данные Дети»: официальный сайт проекта Роскомнадзора [Электронный ресурс] // Режим доступа: URL: http://персональныеданные.дети/o_proekte/

15.Сетевой этикет: как правильно общаться в интернете // Онлайн-школа «Фоксфорд»: официальный сайт // Режим доступа: URL: https://externat.foxford.ru/polezno-znat/setevoy-etiket

16.Цифровой этикет: как правильно общаться в Интернете с коллегами, учениками и родителями [Электронный ресурс] // Российский учебник: официальный сайт // Режим доступа: URL: https://rosuchebnik.ru/material/tsifrovoy-etiket-kak-pravilno-obshchatsya-v-internete/

Календарный план работы

Дата	Мероприятия
01.06.2022	Инструктаж по технике безопасности. Информация и Интернет
02.06.2022	Что такое информационное общество?
03.06.2022	Понятие персональных данных
04.06.2022	Общие рекомендации по обеспечению безопасности в сети Интернет
06.06.2022	Защита информации и кибербезопасность.
07.06.2022	Безопасный серфинг в Интернете
08.06.2022	Как защититься от кибермошенничества. Правила безопасности в киберпространстве
09.06.2022	Безопасное общение в сети Интернет
10.06.2022	Сетевой этикет: как правильно общаться в интернете
14.06.2022	Общение и безопасность в сети Интернет
15.06.2022	Безопасность в сети Wi-Fi
16.06.2022	Как защитить личные данные в сети
17.06.2022	Правила безопасного использования онлайн-сервисов и интернет-ресурсов.
18.06.2022	Потенциально опасные сайты
20.06.2022	Приключения робота Каспера
21.06.2022	Правила безопасного использования мобильных устройств
22.06.2022	Твой безопасный банк в кармане
23.06.2022	Поиск информации в сети Интернет
24.06.2022	Защита от кибер-мошенничества
25.06.2022	Как защититься от кибермошенников: семь правил безопасности в виртуальной среде
27.06.2022	Интернет-зависимость: что это такое и как ее избежать