Утверждаю:

Приказ № 01 от «01» февраля 2024 г.

ИП Черных И.В.

ДОПОЛНИТЕЛЬНАЯ ОБЩЕОБРАЗОВАТЕЛЬНАЯ ОБЩЕРАЗВИВАЮЩАЯ ПРОГРАММА

Безопасный кибермир

Возраст детей: 9 - 15 лет
Срок реализации: 1 месяц

г. Псков
2024 г.

Раздел 1. Пояснительная записка

1.1. Актуальность программы

Цифровая грамотность необходима не только взрослым, но и детям, которые сегодня живут в цифровой эпохе.

Различные игры, приложения, социальные сети и другие виды онлайн-коммуникаций приходят в жизнь детей в самом раннем возрасте. Дети сегодня рано начинают пользоваться компьютером, смартфонами и интернетом. Они становятся активными пользователями цифровых технологий и, таким образом, нуждаются в том, чтобы понимать и избегать рисков, возникающих при использовании этих технологий.

В школе, где многие уроки проводятся с использованием компьютеров и интернета, цифровая грамотность становится еще более важной. Школьники должны уметь не только пользоваться компьютером и интернетом, но и уметь сделать качественную презентацию, и уметь пользоваться разными программами для выполнения школьных заданий, написания рефератов, подготовки проектов.

Цифровая грамотность для детей включает в себя обучение их правилам безопасного использования сети. Одной из главных проблем является доступность нежелательного контента, такого как порнография, насилие, наркотики и т.д. Дети могут случайно наткнуться на такой контент, пытаясь найти информацию для учебы или просто из любопытства. Это может привести к негативным последствиям, таким как психологические проблемы, нарушение поведения и т.д.

Кроме того, дети могут стать жертвами кибербуллинга, когда они подвергаются онлайн-издевательствам со стороны своих сверстников. Это может привести к серьезным проблемам со здоровьем и самооценкой ребенка.

Также существует риск, что дети могут стать жертвами интернет-мошенничества, когда они делятся своими личными данными или финансовой информацией в интернете. Это может привести к краже личных данных, финансовых потерь и другим негативным последствиям.

В целом, цифровая грамотность для детей дает детям уверенность в их способности пользоваться компьютером и интернетом, что поможет им в будущем как в личной жизни, так и в карьере. Знания цифровой грамотности помогут детям быть более конкурентоспособными на рынке труда и успешными в быстро меняющемся мире технологий.

1.2. Направленность программы

Направленность программы - техническая (информационные технологии).

1.3. Цель реализации программы

Целью реализации программы “Безопасный кибермир для подростков” является повышение уровня цифровой грамотности подростков, развитие у них навыков безопасного и ответственного использования цифровых технологий, а также обучение их распознаванию и избеганию потенциальных рисков и угроз в интернете.

1.4. Задачи реализации программы

1. Ознакомление подростков с основами цифровой грамотности и безопасности в киберпространстве.
2. Обучение подростков навыкам критического мышления и оценки информации в интернете.

3. Развитие у подростков умений и навыков безопасного использования различных цифровых инструментов и технологий.
4. Обучение подростков распознаванию и противостоянию кибербуллингу, онлайн-мошенничеству и другим формам интернет-угроз.
5. Информирование подростков о правилах поведения в интернете и ответственности за свои действия в цифровом пространстве.
6. Формирование у подростков навыков безопасного общения и взаимодействия в социальных сетях и других формах онлайн-коммуникации.
7. Обучение подростков основам информационной безопасности и защиты персональных данных в цифровом мире.
8. Создание условий для развития у подростков интереса к изучению основ программирования и информационной безопасности.

1.6. Адресат программы

Возраст обучающихся по программе - от 9 до 15 лет.

Дети в возрасте от 9 до 15 лет являются наиболее уязвимыми для онлайн-рисков и угроз, таких как кибербуллинг, онлайн-хищники, кибермошенники и распространение неприемлемого контента, по нескольким причинам:

- Недостаток критического мышления: Дети этого возраста могут быть менее способны отличать надежный контент от ненадежного, что делает их уязвимыми для манипуляции и эксплуатации.
- Отсутствие понимания рисков: Многие дети не осознают потенциальные риски, связанные с общением с незнакомцами в сети или открытием подозрительных ссылок.
- Большая доступность интернета: В этом возрасте дети имеют легкий доступ к интернету благодаря смартфонам, планшетам и компьютерам, что увеличивает вероятность их контакта с нежелательным контентом или рисками.
- Социальные сети: Социальные сети могут привлекать детей своим игровым характером и возможностью общения с друзьями, но они также могут стать платформой для кибербуллинга и других форм онлайн-агрессии.
- Незащищенность персональных данных: Дети могут не осознавать важность защиты своих личных данных, что может привести к их неправомерному использованию или раскрытию.

  Все это делает необходимым обучение детей цифровой грамотности и безопасному поведению в интернете для защиты их от возможных рисков и угроз.

1.5. Планируемые результаты обучения

В результате обучения у обучающихся будут сформированы следующие навыки:

1. Развитие критического мышления: Подростки научатся оценивать информацию и определять надежные источники, отличать факты от мнений и распознавать манипуляции.
2. Основы безопасности в интернете: Подростки узнают о правилах безопасного использования интернета, научатся отличать безопасный контент от опасного и понимать риски, связанные с определенными видами деятельности в сети.
3. Распознавание мошенничества: Подростки смогут распознавать и предотвращать онлайн-мошенничество, такое как фишинг, вишинг и другие формы киберпреступлений.
4. Безопасное общение: Подростки приобретут навыки безопасного общения в интернете, включая умение противостоять киберзапугиванию, распознавать нежелательные сообщения и прекращать общение с онлайн-хищниками.
5. Защита персональных данных: Подростки поймут важность защиты личных данных и научатся применять соответствующие меры безопасности, такие как использование сложных паролей и двухфакторная аутентификация.
6. Понимание информационной безопасности: Подростки получат знания об основах информационной безопасности, включая понимание принципов работы сетей, атак на системы и методов защиты от них.

1.6. Форма обучения

Форма обучения: очная.

1.7. Режим занятий

Срок реализации программы: 1 месяц, 3 занятия

Количество часов по программе – 6 академических часов.

Занятия проводятся 1 раз в неделю, по 2 академических часа с перерывами между академическими часами 15 минут. В перерыве - физкультминутка и зарядка для глаз.

Академический час равен 40 минутам.

Занятия - групповые, сочетается принцип группового обучения с индивидуальным подходом.

Количество обучающихся в группе - до 10 человек.

Раздел 2. Учебный план программы

№	Наименование разделов (модулей) и тем	Всего ак. часов	Виды учебных занятий, учебных работ		Неделя обучения
			Теор. занятия	Практ. занятия	
1	Тема 1. Основы безопасности в IT	2	2	0	1
2	Тема 2. Психология и безопасность в цифровом мире	2	2	0	2
3	Итоговая аттестация: проверка полученных знаний	2	0	2	3
	Итого	**6**	**4**	**2**	

Раздел 3. Календарный учебный график

Календарный учебный график формируется при осуществлении обучения в течение всего календарного года. По мере набора групп слушателей по программе составляется график, учитывающий объемы лекций, практики, самоподготовки.

Количество занятий: 3 по 2 академических часа.
Количество занятий в неделю: 1

Раздел 4. Рабочая программа

Тема	Виды учебных занятий, учебных работ	Содержание
Тема 1. Основы безопасности в IT		
Урок № 1.	2	1. Вредоносное ПО Что такое вредоносное ПО, каким оно может быть, как попадает на наши устройства. Что делать, чтобы защитить себя. 1.1 Антивирусы Что это такое, как работают и каким функционалом обладают. Какими они бывают и как правильно ими пользоваться.
		2. Аутентификация 2.1 Аутентификация, логины и пароли. Как это работает и почему это важно. Как правильно выбрать пароль. Примеры плохих и хороших паролей. 2.2 Менеджеры паролей. Что это такое, какими бывают и как работают. Можно ли им доверять и как выбрать. 2.3 Двухфакторная аутентификация Что это такое, какие у неё преимущества, какой она бывает, как её настроить.
		3. Электронная почта. Почему она так важна, и как её защитить. 3.1 Письма-вирусы 3.2 Письма-спам 3.3 Черные списки и спам списки. Что это такое, как пользоваться на телефоне и на разных сервисах.
		4. Сайты 4.1 Поддельные сайты. Что это такое, зачем их создают и как их распознать. Примеры фейковых и настоящих сайтов. 4.2 Поддельные ссылки. Какая в них опасность, как распознать и что с ними делать.

		4.3 Сокращенные ссылки. Что это такое и для чего используется. Какие сервисы для этого бывают, примеры. 4.4 Безопасное соединение, протокол HTTPS. Что это, для чего нужен, где он указан.
		5. Приложения 5.1 Установщики приложений и места их получения. Где и как можно безопасно скачать приложение, как его установить. 5.2 Сбор данных приложениями. Какие данные собирают приложения, как можно это проверить и на что обратить внимание. 5.3 Пользование публичными сетями для доступа в приложения и на сайты. 5.4 Геопозиция. Что это, для чего нужно и как не раскрывать её без необходимости. 5.5 Размещение личное информации в соц.сетях и мессенджерах. Личная информация в закрытых чатах или серверах. 5.6 Разрешения для приложений. Что это такое, как контролировать и настраивать.
		6. Конфиденциальные данные 6.1 Опасности хранения конфиденциальных сведений на устройствах, в приложениях и электронной почте. 6.2 Запрос СМС на сайтах. В чем опасность. 6.3 «Бесплатные» предложения. 6.4 Пользование облаками для хранения данных.
Тема 2. Психология и безопасность в цифровом мире		
Урок №2	2	**1. Актуализация темы** 1.1. Обсуждаем кто что смотрит в интернете, вводят ли родители ограничения по пользованию интернетом, нарушают ли они их. 1.2. С какими трудностями ребята уже сталкивались в интернете, их истории и сложности.

		2. Основные ошибки, которые допускают подростки в сети 2.1. Анонимность странички 2.2. Не делиться личным в сети 2.3. Бан/игнор 2.4. Опасные группы 2.5. А если все таки что-то случилось (стыдное/обидное)?
		3. Буллинг в сети 3.1. чем отличается от буллинга в жизни 3.2. почему опаснее чем в жизни 3.3. можно ли избежать? как? 3.4. почему происходит? цели обидчиков 3.5. роли обидчиков, ответственность каждого участвующего человека 3.6. чего не ожидают обидчики 3.7. как действовать если это уже происходит 3.8. когда надо обращаться за помощью к взрослым
Тема 3. Итоговая аттестация: проверка полученных знаний		
Урок №3		Интерактивная игра “Безопасный кибермир”
ИТОГО	**6 ак часов**	

Раздел 5. Оценочные материалы

Реализация программы предусматривает текущий контроль, итоговую аттестацию обучающихся.

Текущий контроль проводится в течение освоения каждой темы программы. Текущий контроль включает следующие формы: наблюдение, ответы на вопросы преподавателя.

Итоговый контроль осуществляется в формате соревнования. Обучающиеся разбирают различные ситуации, связанные с безопасностью в сети интернет, устно отвечают на вопросы интерактивной игры, выбирают ответ из предложенных вариантов.

Раздел 6. Учебно-методические материалы

1. www.saferunet.ru - Центр Безопасного Интернета в России. Сайт посвящен проблеме безопасной, корректной и комфортной работы в Интернете
2. www.friendlyrunet.ru - Фонд "Дружественный Рунет". Фонд поддерживает проекты, связанные с безопасным использованием интернета, содействует российским пользователям, общественным организациям, коммерческим компаниям и государственным ведомствам в противодействии обороту противоправного контента, а также в противодействии иным антиобщественным действиям в Сети
3. www.fid.su/projects/saferinternet/year/hotline/ - Линия помощи "Дети онлайн". Оказание психологической и практической помощи детям и подросткам, которые столкнулись с опасностью или негативной ситуацией во время пользования интернетом или мобильной связью. Линия помощи "Дети онлайн" является первым и единственным такого рода проектом в России и реализуется в рамках Года Безопасного Интернета в России

4. www.microsoft.com - Компания Microsoft разместила на своем интернет ресурсе много полезной информации по безопасности детей в интернете. Заметки и советы, приведенные ниже, помогут вам обеспечить безопасность детей независимо от того, с какой целью они используют интернет: для поиска информации, разработки школьных проектов, игр или беседы с друзьями
5. www.ms-education.ru и www.apkpro.ru - электронный курс программы "Здоровье и безопасность детей в мире компьютерных технологий и Интернет". Программа представляет собой 72-х часовой курс, состоящий из 6 модулей. Каждый модуль программы дает подробное описание и рекомендации по обеспечению безопасной работы детей с компьютером и Интернетом, а также снабжен обширным списком дополнительной литературы и веб-ссылок
6. www.nedopusti.ru - социальный проект по защите прав детей "Не допусти" - социальный проект по защите детей от похищений, сексуальной эксплуатации и жестокого обращения
7. www.za-partoi.ru - "Здоровье школьников" - новый журнал о психологии взросления и физическом развитии детей, о возможностях современной медицины, о взаимоотношениях родителей, детей и учителей, о досуге и здоровом образе жизни
8. www.newseducation.ru - "Большая перемена" сайт для школьников и их родителей
9. www.mirbibigona.ru - "Страна друзей": детская соцсеть: общение, музыка, фотоальбомы, игры, новости
10. www.smeshariki.ru - "Смешарики": развлекательная соцсеть: игры, музыка, мультфильмы
11. www.solnet.ee - "Солнышко": детский портал. Развивающие, обучающие игры для самых маленьких и еще много интересного и для родителей
12. www.1001skazka.com - "1001 сказка". На сайте можно скачать аудиофайлы — сказки, аудиокниги
13. www.nachalka.info - сайт для учащихся начальной школы, родителей и учителей. Здесь можно учиться и играть, развлекаться и закреплять материал школьной программы! Наш сайт создан для того, что бы сделать обучение по школьной программе интереснее и увлекательнее
14. · www.membrana.ru – "Люди. Идеи Технологии". Информационно-образовательный интернет-журнал о новых технологиях
15. www.teremoc.ru - Детский сайт "ТЕРЕМОК" с развивающими играми, загадками, ребусами, мультфильмами
16. www.murzilka.org - Сайт журнала "Мурзилка" со стихами, раскрасками, конкурсами и другой полезной информацией
17. www.e-parta.ru - Блог школьного "Всезнайки" - это ленты новостей по всем школьным предметам, виртуальные экскурсии, психологические и юридические советы по проблемам в школе и на улице, учебные видео-фильмы, обзоры лучших ресурсов Всемирной паутины
18. www.web-landia.ru - Страна лучших сайтов для детей
19. http://www.ligainternet.ru/ - Лига безопасного Интернета
20. http://i-deti.org/ - Портал "Безопасный инет для детей", ресурсы, рекомендации, комиксы
21. http://сетевичок.рф/ - "СЕТЕВИЧОК" сайт для детей — обучение и онлайн-консультирование по вопросам кибербезопасности сетевой безопасности
22. http://www.igra-internet.ru/ — Онлайн интернет-игра "Изучи Интернет – управляй им"
23. http://www.safe-internet.ru/ — сайт Ростелеком "Безопасноть детей в Интернете", библиотека с материалами, памятками, рекомендациями по возрастам

6.2 Материально-техническая и ресурсная база

1. Учебная аудитория на 20 человек.

2. Компьютеры по количеству учащихся и для преподавателя. Требование к компьютеру: Процессор Intel Core i3, Оперативная память минимум — 4 ГБ, Общий объём жестких дисков (HDD):500 ГБ, Операционная система: Windows
3. Интерактивная панель для демонстрации презентаций и игры
4. Выделенная линия интернет 10 Мбит/сек.