Департамент образования Администрации города Омска
бюджетное образовательное учреждение города Омска
«Средняя общеобразовательная школа № 77»

РАССМОТРЕНО
Руководитель ШМО
_____Самойленко Е.Н.
от 23.08.24 дата
№1 протокол

УТВЕРЖДЕНО
Директор
_____КамышниковаО.А.
26.08.24 дата

Дополнительная общеобразовательная общеразвивающая программа
технической направленности
«*Информационная безопасность*»
Срок реализации программы: *1 месяц*
Возраст обучающихся: *7-18 лет*
Трудоемкость программы: *8 часов*
Форма реализации программы: *очная*
Уровень сложности: стартовый

Автор - составитель:
Меркушина Мария Петровна,
педагог дополнительного образования

Омск, 2024

Содержание

Пояснительная записка

Дополнительная общеобразовательная общеразвивающая программа «Информационная безопасность» имеет техническую направленность и предназначена для обучающихся 7-18лет.

Актуальность программы

Актуальность программы "Информационная безопасность" для обучающихся 7-18 лет определяется её современностью и своевременностью, а также соответствием потребностям общества и родителей. В условиях стремительного развития цифровых технологий и увеличения угроз в информационном пространстве, обучение основам информационной безопасности становится необходимым для формирования у обучающихся навыков безопасного поведения в сети. Программа направлена на удовлетворение запросов целевой группы, включая как учащихся, так и их родителей, что делает её особенно актуальной в свете растущего интереса к вопросам защиты личной информации и предотвращения киберугроз. Идеи, придающие программе своеобразие:

Интеграция практических занятий с теоретическими основами, что позволяет учащимся не только усваивать знания, но и применять их на практике.

Использование современных технологий и методик обучения, таких как игровые элементы и симуляции, которые делают процесс обучения более увлекательным и эффективным.

Включение актуальных тем, таких как кибербуллинг, защита личных данных и основы работы с социальными сетями, что соответствует современным вызовам.

Новизна программы

Новизна программы заключается в её комплексном подходе к обучению информационной безопасности. Программа не просто передает знания о существующих угрозах, но и формирует у учащихся критическое мышление, позволяющее им самостоятельно оценивать риски и принимать обоснованные решения в области безопасности. Это делает программу уникальной в контексте образовательных инициатив, направленных на подготовку молодого поколения к жизни в цифровом обществе.

Характеристика целевой группы. Обучающиеся в возрасте от 6 до 18 лет представляют собой разнообразную группу с различными когнитивными и эмоциональными особенностями. Дети 7-10 лет чаще всего нуждаются в визуальных и игровых методах обучения, тогда как обучающиеся 11-17 лет способны к более глубокому анализу информации и самостоятельному решению задач. Важно учитывать, что дети в этом возрасте активно развивают свои социальные навыки, что делает групповую работу особенно эффективной. Детское объединение разновозрастной группы включает детей с различными уровнями подготовки и интересами. Это создает возможность для обмена опытом между старшими и младшими обучающимися, что способствует развитию лидерских качеств у старших и поддерживает мотивацию у младших.

Особенности детей в этой группе могут включать разнообразие в уровне восприятия информации, эмоциональную реакцию на учебный процесс и различные стили обучения. Таким образом, программа "Информационная безопасность" не только отвечает современным требованиям общества, но и учитывает индивидуальные особенности обучающихся.

Форма обучения: очная

Уровень сложности: стартовый.

Форма организации занятий: индивидуальная, групповая, подгрупповая.

Содержание занятий предполагает активное вовлечение детей в процесс обучения через смену видов деятельности. Включение игровых приемов и физкультминуток способствует поддержанию интереса и концентрации обучающихся, что особенно важно для разновозрастной группы. Игровые технологии, применяемые в рамках программы, обеспечивают активное участие детей, способствуют развитию навыков коллаборации и социального взаимодействия, а также помогают создать положительную атмосферу на занятиях. Групповая форма обучения позволяет учитывать разнообразие возрастных особенностей целевой группы. Дети 7-10 лет проявляют высокий интерес к играм и активным действиям, что делает игровые элементы особенно эффективными. Подростки 11-17 лет обладают более развитым критическим мышлением и стремятся к самостоятельности, что открывает возможности для обсуждений и анализа ситуаций в группах. Таким образом, использование групповой формы организации занятий в сочетании с игровыми методами и физической активностью создает динамичную и увлекательную образовательную среду, способствующую успешному усвоению материала и формированию у обучающихся навыков безопасного поведения в цифровом пространстве.

Трудоемкость программы - 8 часов.

Особенности организации образовательного процесса, условия набора и добора обучающихся

Режим занятий - 2 раза в неделю по 40 минут.

На обучение принимаются все желающие без особых навыков и знаний. Наполняемость групп от 10 до 15 человек.

Цель программы:

Формирование у школьников основ знаний в области информационной безопасности, необходимых для защиты личной информации и безопасного взаимодействия в цифровом пространстве посредством освоения программы «Информационная безопасность».

Задачи:

1.Познакомить обучающихся с основными понятиями и принципами информационной безопасности, включая правила безопасного поведения в интернете.

2.Развить навыки анализа потенциальных угроз и методов защиты информации.

3. Научить принимать обоснованные решения при использовании цифровых технологий.

Планируемые результаты:

Личностные:

- проявляет интерес к изучению материала,
- проявляет уважение к личной информации других людей.

Метапредметные

- активно включается в совместную работу с другими обучающимися
- проявляет ответственность за свои действия в цифровом пространстве
- грамотно представляет в интернет-пространстве свои личные и персональные данные.

Результаты по направленности программы:

Знает:

- типы киберугроз,
- методы защиты информации в сети,
- правила безопасного поведения в сети.

Учебно-тематический план

№ п/п	Разделы, тема.	Кол-во часов
1	Введение в информационную безопасность	1
2	Угрозы информационной безопасности	1
3	Защита личной информации	1
4	Безопасное использование паролей	1
5	Мошенничество в Интернете	1
6	Правила безопасного поведения в сети	1
7	Защита от вирусов и вредоносных программ	1
8	Итоговое занятие: практическое применение знаний	1
	Итого	**8 часов**

Содержание программы

Тема 1: Введение в информационную безопасность (1 час)

Форма проведения: Лекция

Вид учебной деятельности: Знакомство с программой, с ТБ на занятиях. Изучение теории: что такое информация и информационная безопасность, выполнение теста по теме.

Формы организации деятельности: групповая и индивидуальная работа

Понятия и термины: Информационная безопасность, конфиденциальность, целостность.

Оценка и контроль: Тестирование по пройденному материалу.

Тема 2: Угрозы информационной безопасности (1 час)

Форма проведения: Семинар

Вид учебной деятельности: Изучение видов угроз информационной безопасности. Обсуждение: где и когда мы можем столкнуться с данными угрозами? Кто уже сталкивался с угрозами.

Формы организации деятельности: Групповая работа

Понятия и термины: Вредоносное ПО, фишинг, социальная инженерия.

Оценка и контроль: Оценка участия в обсуждении, наблюдение.

Тема 3: Защита личной информации (1 час)

Форма проведения: Практическое занятие

Вид учебной деятельности: Практическое применение знаний по защите личной информации. Представление своих примеров по защите личной информации.

Формы организации деятельности: Индивидуальная работа с примерами.

Понятия и термины: Личная информация, конфиденциальность.

Оценка и контроль: Проверка выполненных заданий.

Тема 4: Безопасное использование паролей (1 час)

Форма проведения: Мастер-класс

Вид учебной деятельности: Для чего нужны пароли? Правила выбора паролей. Практическое занятие: создание паролей на различных платформах и в мессенджерах

Формы организации деятельности: Групповая и индивидуальная работа.

Понятия и термины: Пароль, аутентификация.

Оценка и контроль: Оценка качества созданных паролей.

Тема 5: Мошенничество в Интернете (1 час)

Форма проведения: Лекция с элементами дискуссии

Вид учебной деятельности: Изучение теории: Кто такие мошенники? Как распознать мошенника в сети? Обсуждение в группе различных видов мошенничества. Обсуждение темы: как себя обезопасить от мошенников. Ответ на тест.

Формы организации деятельности: Дискуссия в группе.

Понятия и термины: Мошенничество, фишинг.

Оценка и контроль: Тестирование на знание видов мошенничества.

Тема 6: Правила безопасного поведения в сети (1 час)

Форма проведения: Интерактивный урок

Вид учебной деятельности: Изучение этического поведения в сети. Изучение правил поведения в сети. Игра.

Формы организации деятельности: Командная работа.

Понятия и термины: Безопасное поведение, правила сетевой этики.

Оценка и контроль: Оценка участия в игре, наблюдение.

Тема 7: Защита от вирусов и вредоносных программ (1 час)

Форма проведения: Практическое занятие с демонстрацией

Вид учебной деятельности: Что такое вирус? Знакомство с различными видами вирусов. Практическое применение знаний по защите от вирусов.

Формы организации деятельности: Индивидуальная работа с компьютером.

Понятия и термины: Вирусы, антивирусные программы.

Оценка и контроль: Проверка установленных программ на компьютерах.

Тема 8: Итоговое занятие: практическое применение знаний (1 час)

Форма проведения: Проектная работа

Вид учебной деятельности: Создание и презентация проектов по любой изученной теме.

Формы организации деятельности: Групповая работа.

Оценка и контроль: Оценка представленных проектов.

Контрольно-оценочные средства

Для оценки уровня образовательных результатов используются следующие диагностические инструменты:

Тестирование (проверка знаний по темам).

Опрос (устный или письменный).

Наблюдение за участниками (оценка активности на занятиях).

Методы диагностики включают формативное (постоянное) оценивание во время занятий, а также суммативное (итоговое) оценивание на заключительном тестировании.

Применяется балльная система оценивания. В системе оценки используются следующие критерии:

1 балл - обучающийся не усвоил теоретическое содержание программы, допускает ошибки, затрудняется в выполнении практических заданий;

2 балла - обучающийся демонстрирует знание и понимание учебного материала, осознанно применяет знания для решения практических заданий, но иногда допускает некоторые неточности;

3 балла - обучающийся демонстрирует глубокое владение учебным материалом, выполняет качественно все задания.

	Критерии	**Показатели**	**Степень выраженности показателей**	**Баллы**	**Формы, методы, процедуры, инструментарий**
1	**Личностные результаты**				
1.1	Проявляет интерес к изучению материала.	Демонстрирует интереса к изучаемому материалу.	**Высокий** выполнены все задания в установленные сроки. **Средний** выполнена часть заданий; задания выполнены не в срок. **Низкий** не выполнено ни одного задания.	**3** **2** **1**	Наблюдение, опрос, выполнение заданий
1.2	проявляет уважение личной информации других людей	Проявляет уважение к личной информации других людей	**Высокий** с уважением относится к личной информации других. **Средний** не всегда проявляет уважение к личной информации других. **Низкий** не понимает необходимость уважать чужую личную информацию и не проявляет уважения к личной информации других	**3** **2** **1**	Наблюдение, опрос.
2.	**Метапредметные результаты**				

2.1	активно включается в совместную работу с другими обучающимися	Проявляет активность в совместной работе с другими обучающимися	**Высокий** работает активно и дружно с другими обучающимися **Средний** не всегда включается в совместную работу **Низкий** не желает работать совместно с другими обучающимися.	**3** **2** **1**	наблюдение
2.2	проявляет ответственность за свои действия в цифровом пространстве	Демонстрирует ответственное поведение в сети.	**Высокий** в полной мере проявляет ответственность **Средний** не всегда отдает отчет своим действиям в сети **Низкий** не демонстрирует ответственное поведение в сети	**3** **2** **1**	наблюдение
2.3	грамотно представляет в интернет-пространстве свои личные и персональные данные	Представление личных данных в интернете	**Высокий** в полной мере проявляет грамотное представление своих личных данных в сети. **Средний** частично проявляет грамотное представление личных данных **Низкий** не демонстрирует грамотного представления личных данных в сети	**3** **2** **1**	Проверка заданий, наблюдение, опрос
3.	**Предметные результаты**				
3.1	Знает типы киберугроз	Знает основные типы киберугроз	**Высокий** демонстрирует в полной мере знания по теме. **Средний** допускает незначительные ошибки при выполнении заданий. **Низкий** допускает большое количество ошибок при выполнении заданий.	**3** **2** **1**	Выполнение тестов, опрос.
3.2	Знает методы защиты информации в сети	Знает и применяет основные методы защиты информации в сети	**Высокий** знает все основные методы защиты информации в сети. Применяет на практике. **Средний** Знает несколько методов защиты информации в сети, частично применяет на практике **Низкий** плохо ориентируется в методах защиты информации в сети, не проявляет заинтересованность в защите на пракике.	**3** **2** **1**	Выполнение практических заданий, наблюдение, опрос.
3.3	Знает	Знает и проявляет	**Высокий**	**3**	Выполнение

	правила безопасного поведения в сети	правила безопасного поведения в сети	знает и применяет на практике все основные правила поведения в сети. **Средний** Не всегда действует по правилам безопасного поведения в сети. **Низкий** плохо ориентируется в правилах безопасного поведения в сети, на проявляет заинтересованность соблюдать правила.	**2** **1**	практических заданий, наблюдение, опрос

Сводная таблица результатов обучающихся

№ п/п	**ФИО**	**Критерии**							**ИТОГ** (уровень)
		1	**2**	**3**	**4**	**5**	**6**	**7**	
1. **…**									низкий (0-6 б) средний (7-14 б) высокий (15-21 б)

Условия реализации программы

Материально-техническое обеспечение:

- кабинет с доступом к интернету
- ноутбуки (15 шт.)

Информационно-образовательные ресурсы:

- Центр Безопасного Интернета: портал с ресурсами по безопасному использованию интернета, включая советы для родителей и детей https://www.sutori.com/en/story/tsientr-biezopasnogho-intiernieta-v-rossii--xAvk5FaukW8cApyRTGfPziyY
- Линия помощи «Дети онлайн»: психологическая и практическая помощь детям, столкнувшимся с интернет-угрозами http://detionline.com/.
- Электронный курс «Здоровье и безопасность детей в мире компьютерных технологий»: https://nsportal.ru/shkola/sotsialnaya-pedagogika/library/2018/04/03/zdorove-i-bezopasnost-detey-v-mire-kompyuternyh-0.

Учебно-методическое обеспечение:

- презентации по темам
- тесты
- опросники

Кадровые ресурсы: реализацию программы осуществляют педагоги дополнительного образования, имеющие средне-специальное, высшее педагогическое образование, любой квалификации, обладающие компетенциями и навыками:

- владеть формами и методами обучения, в том числе выходящими за рамки учебных занятий.
- использовать и апробировать специальные подходы к обучению всех обучающихся.
- владеть ИКТ-компетентностями.

Список литературы

Нормативно-правовые акты

1. Российская Федерация. Законы. Конституция Российской Федерации : [принята всенародным голосованием 12.12.1993 с изменениями одобренными в ходе общероссийского голосования 01.07.2020]. - Текст : электронный // Консультант плюс : [сайт] – URL: http://www.consultant.ru/document/cons_doc_LAW_28399/ (дата обращения: 08.06.2021).
2. Российская Федерация. Законы. Об образовании в Российской Федерации :Федеральный закон N 273 – ФЗ : [принят Государственной Думой 21 декабря 2012 года : Одобрен Советом Федерации 6 декабря 2012 года]. - Текст : электронный // Консультант плюс : [сайт] – URL: http://www.consultant.ru/document/cons_doc_LAW_140174/ (дата обращения: 08.06.2021).
3. Российская Федерация. Законы. Об основных гарантиях прав ребенка в Российской Федерации: Федеральный закон N 124-ФЗ: [принят Государственной Думой 03 июлю 1998 года : Одобрен Советом Федерации 09 июля 1998 года]. - Текст : электронный // Консультант плюс: [сайт] – URL: http://www.consultant.ru/document/cons_doc_LAW_19558/(дата обращения: 08.06.2021).
4. Российская Федерация. Распоряжения. Концепция развития дополнительного образования детей до 2030 года : Распоряжение от 31 марта 2022 г. № 678-р: [утверждена распоряжением Правительства Российской Федерации от 31 марта 2022 г. № 678-р]. – Текст : электронный // Правительство Российской Федерации: [сайт] – URL: http://government.ru/news/45028/ (дата обращения: 06.04.2022)
5. Российская Федерация. Постановления. Об утверждении санитарных правил СП 2.4.3648-20 «Санитарно-эпидемиологические требования к организациям воспитания и обучения, отдыха и оздоровления детей и молодежи: Постановление Главного государственного санитарного врача РФ от 28.09.2020 N 28: [Зарегистрировано в Минюсте России 18.12.2020 N 61573] – Текст: электронный // Консультант плюс: [сайт] – URL: https://demo.consultant.ru/cgi/online.cgi?req=doc&ts=120496791608760539051969505&cacheid=195B93503245C263A95CB326F2535213&mode=splus&base=RZR&n=371594&rnd=CB5CEFC727FFC7C1549791ACD8F4C2EF#19eje1k71kc (дата обращения: 08.06.2021).

Список литературы для педагогов

1. Баранова, Е.К. Информационная безопасность и защита информации/ Е.К. Баранова. – Москва: РИОР, 2023. – 336с.
2. Бирюков, А. Информационная безопасность: защита и нападение/ А. Бирюков. – Москва: ДМК-ПРЕСС, 2017. – 440 с.
3. Бондарев В.В. Введение в информационную безопасность автоматизированных систем/В. Бондарев. – Москва: МГТУ им. Н.Э.Баумана, 2016. – 252 с.
4. Зенков, А.В. Основы информационной безопасности. Учебное пособие / А.В. Зенков. – Вологда: Инфра-инженерия, 2022. – 104 с.
5. Столлингс, У. Основы защиты сетей. Приложения и стандарты/ У. Столлингс.

– Киев: Вильямс, 2020- 230 с.

Список литературы для родителей и обучающихся

1. Тихоглаз, Ю. Кибер без опасности/ Ю. Тихоглаз. – Москва: Белая ворона, 2024 – 112 с.
2. Шарова, Л.В. Безопасный интернет/ Л.В. Шарова. – Ростов-на – Дону: Феникс-премьер, 2021 – 80 с.