

РАССМОТРЕНО

на заседании МО №1

от 31.08.2020

Председатель МО



ПРОВЕРЕНО

Зам.директора по УВР



Малафеева Е.А.

УТВЕРЖДАЮ

Директор ГКОУ для детей-

сирот г.о. Чапаевск



Калабекова Н.А.

Приказ № 250/1 от 31.08.20

РАБОЧАЯ ПРОГРАММА

по внеурочной деятельности

«Информационная безопасность»

для обучающихся 8 класса с задержкой психического развития

на 2020-2021 учебный год

Основными целями изучения курса «Информационная безопасность» являются:

- обеспечение условий для профилактики негативных тенденций в информационной культуре учащихся, повышения защищенности детей от информационных рисков и угроз;
- формирование навыков своевременного распознавания онлайн-рисков (технического, контентного, коммуникационного, потребительского характера и риска интернетзависимости).

Задачи программы:

- сформировать общекультурные навыки работы с информацией (умения, связанные с поиском, пониманием, организацией, архивированием цифровой информации и ее критическим осмыслением, а также с созданием информационных объектов с использованием цифровых ресурсов (текстовых, изобразительных, аудио и видео);
- создать условия для формирования умений, необходимых для различных форм коммуникации (электронная почта, чаты, блоги, форумы, социальные сети и др.) с различными целями и ответственного отношения к взаимо-действию в современной информационно-телекоммуникационной среде;
- сформировать знания, позволяющие эффективно и безопасно использовать технические и программные средства для решения различных задач, в том числе использования компьютерных сетей, облачных сервисов и т.п.;
- сформировать знания, умения, мотивацию и ответственность, позволяющие решать с помощью цифровых устройств и интернета различные повседневные задачи, связанные с конкретными жизненными ситуациями, предполагающими удовлетворение различных потребностей;
- сформировать навыки по профилактике и коррекции зависимого поведения школьников, связанного с компьютерными технологиями и Интернетом.

Результаты освоения курса внеурочной деятельности

Предметные:

Выпускник научится:

- ☐ анализировать доменные имена компьютеров и адреса документов в интернете;
- ☐ безопасно использовать средства коммуникации,
- ☐ безопасно вести и применять способы самозащиты при попытке мошенничества,
- ☐ безопасно использовать ресурсы интернета.

Выпускник овладеет:

- ☐ приемами безопасной организации своего личного пространства данных с использованием индивидуальных накопителей данных, интернет-сервисов и т.п.

Выпускник получит возможность овладеть:

- ☐ основами соблюдения норм информационной этики и права;
- ☐ основами самоконтроля, самооценки, принятия решений и осуществления осознанного выбора в учебной и познавательной деятельности при формировании современной культуры безопасности жизнедеятельности;
- ☐ использовать для решения коммуникативных задач в области безопасности жизнедеятельности различные источники информации, включая Интернет-ресурсы и другие базы данных.

Метапредметные.

Регулятивные универсальные учебные действия.

В результате освоения учебного курса обучающийся сможет:

- ☐ идентифицировать собственные проблемы и определять главную проблему;
- ☐ выдвигать версии решения проблемы, формулировать гипотезы, предвосхищать конечный результат;

- ☐ ставить цель деятельности на основе определенной проблемы и существующих возможностей;
- ☐ выбирать из предложенных вариантов и самостоятельно искать средства/ресурсы для решения задачи/достижения цели;
- ☐ составлять план решения проблемы (выполнения проекта, проведения исследования);
- ☐ описывать свой опыт, оформляя его для передачи другим людям в виде технологии решения практических задач определенного класса;
- ☐ оценивать свою деятельность, аргументируя причины достижения или отсутствия планируемого результата;
- ☐ находить достаточные средства для выполнения учебных действий в изменяющейся ситуации и/или при отсутствии планируемого результата;
- ☐ работая по своему плану, вносить коррективы в текущую деятельность на основе анализа изменений ситуации для получения запланированных характеристик продукта/результата;
- ☐ принимать решение в учебной ситуации и нести за него ответственность.

Познавательные универсальные учебные действия.

В результате освоения учебного курса обучающийся сможет:

- ☐ выделять явление из общего ряда других явлений;
- ☐ определять обстоятельства, которые предшествовали возникновению связи между явлениями, из этих обстоятельств выделять определяющие, способные быть причиной данного явления, выявлять причины и следствия явлений;
- ☐ строить рассуждение от общих закономерностей к частным явлениям и от частных явлений к общим закономерностям;
- ☐ излагать полученную информацию, интерпретируя ее в контексте решаемой задачи;
- ☐ самостоятельно указывать на информацию, нуждающуюся в проверке, предлагать и применять способ проверки достоверности информации;
- ☐ критически оценивать содержание и форму текста;
- ☐ определять необходимые ключевые поисковые слова и запросы.

Коммуникативные универсальные учебные действия.

В результате освоения учебного курса обучающийся сможет:

- ☐ строить позитивные отношения в процессе учебной и познавательной деятельности;
- ☐ критически относиться к собственному мнению, с достоинством признавать ошибочность своего мнения (если оно таково) и корректировать его;
- ☐ договариваться о правилах и вопросах для обсуждения в соответствии с поставленной перед группой задачей;
- ☐ делать оценочный вывод о достижении цели коммуникации непосредственно после завершения коммуникативного контакта и обосновывать его.
- ☐ целенаправленно искать и использовать информационные ресурсы, необходимые для решения учебных и практических задач с помощью средств ИКТ;
- ☐ выбирать, строить и использовать адекватную информационную модель для передачи своих мыслей средствами естественных и формальных языков в соответствии с условиями коммуникации; использовать компьютерные технологии (включая выбор адекватных задаче инструментальных программно-аппаратных средств и сервисов) для решения информационных и коммуникационных учебных задач, в том числе: вычисление, написание писем, сочинений, докладов, рефератов, создание презентаций и др.;
- ☐ использовать информацию с учетом этических и правовых норм;
- ☐ создавать информационные ресурсы разного типа и для разных аудиторий, соблюдать информационную гигиену и правила информационной безопасности.

Личностные.

- ☐ осознанное, уважительное и доброжелательное отношение к окружающим людям в реальном и виртуальном мире, их позициям, взглядам, готовность вести диалог с другими людьми, обоснованно осуществлять выбор виртуальных собеседников;
- ☐ готовность и способность к осознанному выбору и построению дальнейшей индивидуальной траектории образования на базе ориентировки в мире профессий и профессиональных предпочтений, с учетом устойчивых познавательных интересов;
- ☐ освоенность социальных норм, правил поведения, ролей и форм социальной жизни в группах и сообществах;

□ сформированность понимания ценности безопасного образа жизни; интериоризация правил индивидуального и коллективного безопасного поведения в информационно-телекоммуникационной среде.

Критерии оценивания планируемых результатов программ внеурочной деятельности.

По программам внеурочной деятельности применяется безотметочная система оценивания.

Сроки реализации программы

Программа внеурочной деятельности «Информационная безопасность» предназначена для обучающихся 8 класса, все занятия по внеурочной деятельности проводятся после всех уроков основного расписания, продолжительность соответствует рекомендациям СанПиН. Данная программа составлена в соответствии с возрастными особенностями обучающихся и рассчитана на проведение в 8-м классе 1 час в неделю (34 часов в год);

Содержание курса внеурочной деятельности с указанием форм организации и видов деятельности

Содержание программы учебного курса соответствует темам примерной основной образовательной программы основного общего образования (ПООП ООО) по учебным предметам «Информатика» и «Основы безопасности жизнедеятельности», а также расширяет их за счет привлечения жизненного опыта обучающихся в использовании всевозможных технических устройств (персональных компьютеров, планшетов, смартфонов и пр.), позволяет правильно ввести ребенка в цифровое пространство и корректировать его поведение в виртуальном мире.

Основное содержание программы представлено разделами «Безопасность общения», «Безопасность устройств», «Безопасность информации».

Каждый раздел учебного курса завершается выполнением проектной работы по одной из тем, предложенных на выбор учащихся.

В преподавании курса «Цифровая гигиена» используются разнообразные формы обучения: традиционный урок (коллективная и групповая формы работы), тренинги (в классической форме или по кейс-методу), дистанционное обучение (электронные курсы, видеоролики, почтовые рассылки, смешанный формат.

Содержание учебного курса

Раздел 1. «Безопасность общения»

Тема 1. Общение в социальных сетях и мессенджерах. С кем безопасно общаться в интернете. 1 час. Социальная сеть. История социальных сетей.

Мессенджеры. Назначение

социальных сетей и мессенджеров. Пользовательский контент.

Персональные данные как основной капитал личного пространства в цифровом мире. Правила добавления друзей в социальных сетях. Профиль пользователя. Анонимные социальные сети.

Тема 2. Пароли для аккаунтов социальных сетей. Безопасный вход в аккаунты. 1 час.

Сложные пароли. Онлайн генераторы паролей. Правила хранения паролей. Использование функции браузера по запоминанию паролей. Виды аутентификации. Настройки безопасности аккаунта. Работа на чужом компьютере с точки зрения безопасности личного аккаунта.

Тема 3. Настройки конфиденциальности в социальных сетях. 1 час. Настройки приватности и конфиденциальности в разных социальных сетях. Приватность и конфиденциальность в мессенджерах.

Тема 4. Публикация информации в социальных сетях. 1 час.

Персональные данные. Публикация личной информации.

Тема 5. Кибербуллинг. 1 час.

Определение кибербуллинга. Возможные причины кибербуллинга и как его избежать? Как не стать жертвой кибербуллинга. Как помочь жертве кибер-буллинга.

Тема 6. Публичные аккаунты. Фишинг. 1 час.

Настройки приватности публичных страниц. Правила ведения публичных страниц. Овершеринг. Фишинг как мошеннический прием. Популярные варианты распространения фишинга. Отличие настоящих и фишинговых сайтов. Как защититься от фишеров в социальных сетях и мессенджерах.

Выполнение и защита индивидуальных и групповых проектов 1 час.

Характеристика видов деятельности:

Выполняет базовые операции при использовании мессенджеров и социальных сетей.

Создает свой образ в сети Интернет. Изучает историю и социальную значимость личных аккаунтов в сети Интернет.

Руководствуется в общении социальными ценностями и установками коллектива и общества в целом. Изучает правила сетевого общения.

Изучает основные понятия регистрационной информации и шифрования.

Умеет их применить. Объясняет причины использования безопасного входа при работе на чужом устройстве. Демонстрирует устойчивый навык безопасного входа.

Раскрывает причины установки закрытого профиля. Меняет основные настройки приватности в личном профиле. Осуществляет поиск и использует информацию, необходимую для выполнения поставленных задач. Реагирует на опасные ситуации, Распознает провокации и попытки манипуляции со стороны виртуальных собеседников.

Решает экспериментальные задачи.

Самостоятельно создает источники информации разного типа и для разных аудиторий, соблюдая правила информационной безопасности.

Анализ проблемных ситуаций.

Раздел 2. «Безопасность устройств»

Тема 1. Что такое вредоносный код. 1 час.

Виды вредоносных кодов. Возможности и деструктивные функции вредоносных кодов.

Тема 2. Распространение вредоносного кода. 1 час.

Способы доставки вредоносных кодов. Исполняемые файлы и расширения вредоносных кодов. Вредоносная рассылка. Вредоносные скрипты. Способы выявления наличия вредоносных кодов на устройствах. Действия при обнаружении вредоносных кодов на устройствах.

Тема 3. Методы защиты от вредоносных программ. 1 час.

Способы защиты устройств от вредоносного кода. Антивирусные программы и их характеристики. Правила защиты от вредоносных кодов.

Тема 4. Распространение вредоносного кода для мобильных устройств. 1 час.

Расширение вредоносных кодов для мобильных устройств. Правила безопасности при установке приложений на мобильные устройства.

Выполнение и защита индивидуальных и групповых проектов. 1 часа.

Характеристика основных видов деятельности:

Соблюдает технику безопасности при эксплуатации компьютерных систем.
Использует инструментальные программные средства и сервисы адекватно задаче. Выявляет и анализирует (при помощи чек-листа) возможные угрозы информационной безопасности объектов.
Изучает виды антивирусных программ и правила их установки.
Разрабатывает презентацию, инструкцию по обнаружению, алгоритм установки приложений на мобильные устройства для учащихся более младшего возраста. Умеет работать индивидуально и в группе. Принимает позицию собеседника, понимая позицию другого, различает в его речи: мнение (точку зрения), доказательство (аргументы), факты; гипотезы, аксиомы, теории.

Раздел 3 «Безопасность информации»

Тема 1. Социальная инженерия: распознать и избежать. 1 час. Приемы социальной инженерии. Правила безопасности при виртуальных контактах.

Тема 2. Ложная информация в Интернете. Безопасность при использовании платежных карт в Интернете. 1 час.

Цифровое пространство как площадка самопрезентации, экспериментирования и освоения различных социальных ролей. Фейковые новости. Поддельные страницы.

Транзакции и связанные с ними риски. Правила совершения онлайн покупок. Безопасность банковских сервисов.

Тема 3. Беспроводная технология связи. Резервное копирование данных. 1 час.

Уязвимость Wi-Fi-соединений. Публичные и непубличные сети. Правила работы в публичных сетях.

Безопасность личной информации. Создание резервных копий на различных устройствах.

Тема 4. Основы государственной политики в области формирования культуры информационной безопасности. 1 час.

Доктрина национальной информационной безопасности. Обеспечение свободы и равенства доступа к информации и знаниям. Основные направления государственной политики в области формирования культуры информационной безопасности.

Выполнение и защита индивидуальных и групповых проектов. 1 часа.

Характеристика основных видов деятельности:

Находит нужную информацию в базах данных, составляя запросы на поиск.

Систематизирует получаемую информацию в процессе поиска.

Определяет возможные источники необходимых сведений, осуществляет поиск информации. Отбирает и сравнивает материал по нескольким источникам. Приводит примеры рисков,

Связанных с совершением онлайн покупок (умеет определить источник риска).

Разрабатывает возможные варианты решения ситуаций, связанных с рисками использования платежных карт в Интернете. Используя различную информацию, определяет понятия. Изучает особенности и стиль ведения личных и публичных аккаунтов.

Календарно-тематическое планирование

№ занятия	Дата занятия	Количество часов	Тема
Раздел 1. «Безопасность общения»			
1		1	Общение в социальных сетях и мессенджерах.
2		1	С кем безопасно общаться в интернете
3		1	Пароли для аккаунтов социальных сетей.
4		1	Безопасный вход в аккаунты.
5		1	Настройки конфиденциальности в социальных сетях.
6		1	Публикация информации в социальных сетях.
7		1	Кибербуллинг
8		1	Публичные аккаунты
9-10		2	Фишинг
11-13		3	Выполнение и защита индивидуальных и групповых проектов
Раздел 2. «Безопасность устройств»			
14		1	Что такое вредоносный код
15		1	Распространение вредоносного кода.
16-17		2	Методы защиты от вредоносных программ.
18		1	Распространение вредоносного кода для мобильных устройств.
19-21		3	Выполнение и защита индивидуальных и групповых проектов
Раздел 3 «Безопасность информации»			
22		1	Социальная инженерия: распознать и избежать.
23		1	Ложная информация в Интернете.
24		1	Безопасность при использовании платежных карт в Интернете.
25		1	Беспроводная технология связи.
26		1	Резервное копирование данных.
27-28		2	Основы государственной политики в области формирования культуры информационной безопасности.
29-31		3	Выполнение и защита индивидуальных и групповых проектов.
32-34		3	Повторение