

**Аннотация к рабочей программе по информационной безопасности
кибербезопасности 7-8 класс (ТНР)**

<p>Название программы</p>	<p>Программа по информационной безопасности и кибербезопасности составлена с учетом особенностей детей с ТНР, испытывающих стойкие трудности в обучении и требующих специальной коррекционно-развивающей направленности образовательного процесса. Повышенная истощаемость центральной нервной системы и в связи с этим сниженная познавательная активность и работоспособность, недостаточность произвольного внимания, пространственной ориентировки, плохо развитые навыки самостоятельной работы и самоконтроля, инертность психических процессов, слабая память - все эти и другие особенности учащихся с ТНР отрицательно влияют на успешность обучения и являются основной причиной их стойкой неуспеваемости в учебе.</p>
<p>Цели изучения предмета</p>	<p>Для достижения поставленной цели решаются следующие корректирующие задачи: Формирование у учащихся цифровой и информационной культуры; Воспитание у учащихся нравственности и культуры взаимоотношения с людьми на основе общечеловеческих ценностей в сети «Интернет»; Утверждение в сознании и чувствах учащихся правильных моделей поведения, ценностей, взглядов и убеждений для успешной жизнедеятельности учащегося в сети «Интернет»; Углубление знаний учебных дисциплин «Информатика», «ОБЖ» и «Обществознание» в процессе обучения в рамках программы; Интеллектуальное развитие учащихся, формирование творческих и прикладных качеств мышления; Развитие интереса к различным сферам информационных технологий; Совершенствование навыков самообразования, всестороннего развития и социализации; Обучение поиску и отбору информации, её интерпретации и применимости; Развитие логического мышления, умений обобщения и конкретизации, анализа и синтеза; Воспитание умения трудиться, самостоятельности, ответственности и творческого отношения к учёбе; Обучающие: Сформировать систему знаний в сфере обществознания, информационных технологий и основ безопасности жизнедеятельности; Обучить элементам системного мышления использовать инструменты активизации мышления; Отработка навыков и умений для безопасного и полезного использования информационных технологий: сравнение информации, критический анализ, выделение главных мыслей и грамотное изложение, а также восприятия и усвоения информации из сети «Интернет». Развивающие: Развить интеллектуальные и социальные способности обучающихся; Развить навыки сетевого общения и коммуникации в сети «Интернет», поиска и работы с информацией, обеспечения безопасности цифровых устройств и аккаунтов при осуществлении сетевых покупок; Развить деловые и гражданские качества, такие как самостоятельность,</p>

	<p>ответственность, активность и аккуратность; Сформировать потребности в самопознании и саморазвитии.</p> <p>Воспитательные:</p> <p>Воспитать культуру общения и поведения в сетевом пространстве; Воспитать целеустремлённость личности; Воспитать толерантную и культурную личность; Воспитать правильный образ гражданина.</p>
Место учебного предмета в учебном плане	На изучение информационной безопасности. Кибербезопасности отводится 1 час в неделю с 7 по 8 класс (34 часа за год в каждом классе, всего 68 часов).
Содержание программы	<p>7 класс</p> <p>Модуль 1. Общие сведения о безопасности ПК и Интернета (5 часов). Как работают мобильные устройства. Угрозы для мобильных устройств. Распространение вредоносных файлов через приложения для смартфонов и планшетов(скачивание фотографий, музыки, игр). Виды защиты киберпространства (что такое несанкционированный доступ, разрушение и утрата информации, искажение информации). Кто обеспечивает защиту киберпространства. Что такое геоинформационные системы (ГИС). Глобальные информационные Сети стихийным бедствиям.</p> <p>Модуль 2. Техника безопасности и экология (5 часов). Компьютер и мобильные устройства в чрезвычайных ситуациях. Дополнения к ДТП. Компьютер и мобильные (сотовые) устройства в правилах безопасности. Компьютеры и мобильные устройства в экстремальных условиях. Везде ли есть Интернет. ТБ при работе с мобильными устройствами. Первая помощь при проблемах в интернете (службы помощи). Воздействие радиоволн на здоровье и окружающую среду (Wi-Fi, Bluetooth, GSM).</p> <p>Модуль 3. Проблемы Интернет-зависимости (2 часа). Виды Интернет-зависимости. Компьютер и зрение.</p> <p>Модуль 4. Методы обеспечения безопасности ПК и Интернета. Вирусы и антивирусы (8 часов). Вирусы и антивирусы. Как распространяются вирусы. Источники и причины заражения. Скорая компьютерная помощь. Признаки заражения компьютера. Что такое антивирусная защита. Как лечить компьютер. Защита мобильных устройств. Как защитить данные от потерь. Копирование и восстановление. Всегда ли можно спасти свои данные. Защита файлов. Что такое право доступа.</p>

Защита детей в социальных сетях. ПО для родителей. Ограничение времени нахождения в сети.

Модуль 5. Мошеннические действия в Интернете. Киберпреступления (2 часа).

Опасности мобильной связи. Предложения по установке вредоносных приложений.

Мошеннические СМС.

Прослушивание разговоров. Определение местоположения телефона.

Модуль 6. Сетевой этикет. Психология и сеть (10 часов).

Что такое личные данные. Все, что выложено в Интернет, может стать известно всем.

«Лишняя информация» о себе и других в Интернете. Какая информация принадлежит вам. Анонимность в сети.

Что такое этикет. Виды этикета (личный, деловой, письменный, дискуссионный и пр.).

Различия этикета в разных странах.

Как появился нетикет, что это такое. Общие правила сетевого этикета.

Личное общение и общение в группе – чем они отличаются (чаты, форумы, службамгновенных сообщений).

Этика дискуссий. Взаимное уважение при интернет-общении. Этикет и безопасность. Эмоции в сети, их выражение.

Реальная и виртуальная личность, реальные встречи с виртуальными знакомыми и их опасность, угрозы и оскорбления – чем это может закончиться.

Если вы стали жертвой компьютерной агрессии: службы помощи.

Модуль 7. Правовые аспекты защиты киберпространства (2 часа).

Собственность в Интернете. Авторское право. Интеллектуальная собственность. Платная и бесплатная информация.

Обобщение материала курса. Игра-квест «Знатоки кибербезопасности».

8 класс

Модуль 1. Общие сведения о безопасности ПК и Интернета (5 часов).

Информационная безопасность

Защита персональных данных, почему она нужна. Категории персональных данных.

Биометрические персональные данные.

Источники данных в Интернете: почта, сервисы обмена файлами и др.

Хранение данных в Интернете.

Возможности и проблемы социальных сетей.

Безопасный профиль в социальных сетях. Составление сети контактов.

Модуль 2. Техника безопасности и экология (2 часа).

Комплекс упражнений при работе за компьютером.

Воздействие на зрение ЭЛТ, жидкокристаллических, светодиодных, монохромных мониторов.

Модуль 3. Проблемы Интернет-зависимости (3 часа).

Для чего может быть полезен ПК и Интернет (развивающие игры,

	<p>обучение, общение и т.п.)и как польза превращается во вред. Киберкультура (массовая культура в сети) и личность. Психологическое воздействие информации на человека. Управление личностью через сеть.</p> <p>Модуль 4. Методы обеспечения безопасности ПК и Интернета. Вирусы и антивирусы (16 часов). Защита файлов. Права пользователей. Защита при загрузке и выключении компьютера.Безопасность при скачивании файлов. Безопасность при просмотре фильмов онлайн. Защита программ и данных от несанкционированного копирования. Организационные, юридические, программные и программно-аппаратные меры защиты. Защита программ и данных с помощью паролей, программных и электронных ключей, серийных номеров, переноса в онлайн и т.п. Неперемещаемые программы. Методы защиты фото и видеоматериалов от копирования в сети. Защита от копирования контента сайта. Как развивались вирусы. Могут ли вирусы воздействовать на аппаратуру ПК. Как вирусы воздействуют на файлы. Проверка на наличие вирусов. Сканеры и др. Может ли вирус воздействовать на рабочий стол.Источники заражения ПК. Антивирусное ПО, виды и назначение. Методы защиты от вирусов. Как распознаются вирусы.</p> <p>Модуль 5. Мошеннические действия в Интернете. Киберпреступления (4 часа). Утечка и обнародование личных данных. Подбор и перехват паролей. Взломы аккаунтов в социальных сетях. Виды мошенничества в Интернете. Фишинг (фарминг). Азартные игры. Онлайн-казино. Букмекерские конторы. «инвестирования» денег. Выигрыш в лотерею.</p> <p>Модуль 6. Сетевой этикет. Психология и сеть (1 час). Психологическая обстановка в Интернете: грифинг, кибербуллинг, кибер-моббинг, троллинг, буллицид.</p> <p>Модуль 7. Правовые аспекты защиты киберпространства (3 часа). Защита прав потребителей при использовании услуг Интернет.Защита прав потребителей услуг провайдера. Обобщение материала курса. Игра-квест «Знатоки кибербезопасности».</p>
Список приложений	<p>УЧЕБНО-МЕТОДИЧЕСКОЕ ОБЕСПЕЧЕНИЕ ОБРАЗОВАТЕЛЬНОГО ПРОЦЕССА</p> <ol style="list-style-type: none"> 1. Персональный компьютер (ОС Winsows). 2. Ноутбук-трансформер мобильного класса (ACER TravelMate Spin B3) 3. Интерактивная доска. 4. Многофункциональное устройство (МФУ) сканер, принтер (XEROX)

	<p>5. Компьютерная мышь (Aceline CM 904BU, Aceline CM 906BU, Aceline CM 503BU, Aceline CM 408BU, Aceline CM 407BU).</p> <p>4. Прикладное (специальное) программное обеспечение.</p> <p>5. Устройства вывода звуковой информации.</p> <p>6. Устройства для записи (ввода) звуковой информации.</p> <p>7. Устройства ввода текстовой и графической информации.</p> <p>Методические материалы</p> <p>1. Методическое пособие для учителя к учебникам М. С. Цветковой</p> <p>2. Портал Международного квеста по цифровой грамотности www.Сетевичок.рф https://toipkro.ru/content/files/documents/podrazdeleniya/ordo/ciber%20bezopasnost.pdf</p>
--	--

ДОКУМЕНТ ПОДПИСАН ЭЛЕКТРОННОЙ ПОДПИСЬЮ

**МУНИЦИПАЛЬНОЕ БЮДЖЕТНОЕ ОБЩЕОБРАЗОВАТЕЛЬНОЕ
УЧРЕЖДЕНИЕ ГРЯЗОВЕЦКОГО МУНИЦИПАЛЬНОГО ОКРУГА
ВОЛОГОДСКОЙ ОБЛАСТИ "СРЕДНЯЯ ШКОЛА № 2 Г.ГРЯЗОВЦА", Шахова**
Светлана Ивановна, Директор

15.09.23 13:23 (MSK)

Сертификат E8C1693AB6292D8BF0C3E02436A0AC2F