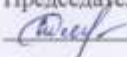


государственное бюджетное общеобразовательное учреждение Самарской области
основная общеобразовательная школа имени Героя Советского Союза М.М.Медведева
с.Коноваловка муниципального района Борский Самарской области

Рассмотрено на МО учителей
Председатель МО

 Т.А.Дмитриева

Протокол №1 от 29.08.2019

Согласовано
Завуч по УВР

 Л.Ш.Буханцова

Утверждено
Директор школы

 М.Г.Соболева

Приказ № 1/7-од от 30.08.2019

Программа

внеурочной деятельности

«Цифровая гигиена»

(модифицированная)

для обучающихся 7 – 8 классов

на 2019-2020 учебный год

направление «Общеинтеллектуальное»

Учитель: Буханцова Л.Ш.

с.Коноваловка, 2019

ПОЯСНИТЕЛЬНАЯ ЗАПИСКА

Рабочая программа внеурочной деятельности «Цифровая гигиена» по общеинтеллектуальному направлению составлена на основе:

- Федерального государственного образовательного стандарта основного общего образования,
- Основной образовательной программы основного общего образования ГБОУ ООШ с.Коноваловка на 2019-2020 учебный год,
- Учебного плана внеурочной деятельности ГБОУ ООШ с.Коноваловка.

Основными целями изучения курса «Цифровая гигиена» 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 интернет-зависимости).

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 взаимодействию 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.

ЛИЧНОСТНЫЕ, МЕТАПРЕДМЕТНЫЕ И ПРЕДМЕТНЫЕ РЕЗУЛЬТАТЫ ОСВОЕНИЯ КУРСА «ЦИФРОВАЯ ГИГИЕНА»

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.

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.

МЕСТО ПРЕДМЕТА «ЦИФРОВАЯ ГИГИЕНА» В УЧЕБНОМ ПЛАНЕ

Программа курса «Цифровая гигиена» адресована учащимся 7-8 классов. Общее число учебных часов за год обучения составляет 34 часа (1 ч в неделю).

СОДЕРЖАНИЕ КУРСА «ЦИФРОВАЯ ГИГИЕНА

Раздел 1: Информация. Информационная сфера. Информационная безопасность. Национальные интересы и безопасность России. **Самостоятельная работа:** составление тестов к разделу «Основные понятия и определения, эволюция подходов к обеспечению информационной безопасности»

Раздел 2: Информационная война. Информационное оружие. Угрозы безопасности России. Угрозы безопасности АСОД.

Раздел 3: Показатели защищенности СВТ. Защита информации в АСОД. Виды доступа. Уровни доступа. Контроль доступа

Лабораторная работа «Идентификация и аутентификация пользователя»

Практическая работа «Основные методы и приемы защиты от несанкционированного доступа»

Самостоятельная работа: «Работа с конспектом лекций – составление тестов к разделу «Защита от несанкционированного доступа, модели и основные принципы защиты информации»

Раздел 4: Проблема вирусного заражения программ. Структура современных вирусных программ. Перспективные методы антивирусной защиты. Основные классы антивирусных программ.

Практическая работа: Особенности закладок и защита от воздействия закладок. Пакеты антивирусных программ

Самостоятельная работа: Составление таблиц для систематизации учебного материала.

Раздел 5: Криптографические методы защиты информации. Проблемы защиты информации в сетях ЭВМ.

Практические работы: Перехват вывода на экран, перехват ввода с клавиатуры. Перехват и обработка файловых операций. Защита информации от копирования. Защита программ в оперативной памяти.

Самостоятельная работа: составление математической модели, алгоритма и программы шифрации историческими шифрами

Раздел 6: Организационная защита информации. Комплексное обеспечение безопасности. Правовые основы защиты информации

ТЕМАТИЧЕСКОЕ ПЛАНИРОВАНИЕ

№ п/п	Тема	Кол-во часов
1	Раздел 1. Основные понятия и определения, эволюция подходов к обеспечению информационной безопасности	4
2	Раздел 2. Информационные, программно-математические, физические и организационные угрозы	2
3	Раздел 3. Защита от несанкционированного доступа, модели и основные принципы защиты информации	7
4	Раздел 4. Компьютерные вирусы и антивирусные программы	7
5	Раздел 5. Защита от утечки информации по техническим каналам	11
6	Раздел 6. Организационно-правовое обеспечение информационной безопасности	3
	Итого:	34

ПЛАНИРУЕМЫЕ РЕЗУЛЬТАТЫ

В ходе проведения программы участники занятий должны овладеть компетенциями, способствующими обеспечению их информационно-психологической безопасности, а именно:

- владеть знаниями о интернет-рисках и угрозах в информационном пространстве;
- обладать выраженной мотивационной направленностью на поддержание ответственной позиции при пользовании информационно-коммуникационными технологиями;
- уметь анализировать и критически относиться к информации в информационно-коммуникационных сетях;
- определять наличие негативного, недостоверного, небезопасного содержания в интернет-контенте;
- владеть и применять эффективные способы и приёмы защиты от нежелательной информации и контактов в интернете;
- определять манипулятивные проявления и намерения в потребительском сегменте интернет-пространства;
- владеть нормами интернет-этикета, приёмами эффективной коммуникации, руководствоваться принципами уважительного и толерантного отношения к другим пользователям при взаимодействии в сети Интернет.

ОПИСАНИЕ УЧЕБНО-МЕТОДИЧЕСКОГО ОБЕСПЕЧЕНИЯ

1. Бабаш А.В. Информационная безопасность: Лабораторный практикум / А.В. Бабаш, Е.К. Баранова, Ю.Н. Мельников. – М.: КноРус, 2019. – 432 с
2. Вехов В. Б. Компьютерные преступления: способы совершения и раскрытия / В.Б. Вехов; Под ред. акад. Б.П. Смагоринского. – М.: Право и закон, 2014. – 182 с.
3. Громов Ю.Ю. Информационная безопасность и защита информации: Учебное пособие / Ю.Ю. Громов, В.О. Драчев, О.Г. Иванова. – Ст. Оскол: ТНТ, 2017. – 384 с.
4. Дети в информационном обществе // <http://detionline.com/journal/about>