

Государственное бюджетное общеобразовательное учреждение Самарской области основная общеобразовательная школа с. Верхнее Санчелеево муниципального района Ставропольский Самарской области

Согласовано
Протокол № 8 Методического Совета
от «27» июня 2024 г.

Утверждено
Директор ГБОУ ООШ с. Верхнее Санчелеево
Приказ № 194-од от «27» июня 2024 г.
Н.П. Безроднова



C=RU, O=ГБОУ
ООШ с.
Верхнее
Санчелеево,
CN=Безродн
ова Наталья
Петровна,
E=bezrodnova
197_9@mail.ru
2023.10.05
10:11:
25+04'00'

**Рабочая программа
внеурочной деятельности
«Информационная безопасность»
(обеспечение безопасности жизни и здоровья
обучающихся)**

Составитель: учитель информатики
Дергунова Ж.Ю.

СОДЕРЖАНИЕ

Пояснительная записка	3
Содержание обучения	5
Планируемые результаты освоения программы	8
Тематическое планирование	11
Учебно-методическое обеспечение образовательного процесса	11

ПОЯСНИТЕЛЬНАЯ ЗАПИСКА

Данная программа составлена на основе курса «Информационная безопасность» для общеобразовательных организаций авторов Тонких И.М., Комарова М.М., Ледовского В.И., Михайлова А.В., переработана и модифицирована.

Развитие информационного общества предполагает внедрение информационных технологий во все сферы жизни, но это означает и появление новых угроз безопасности – от утечек информации до кибертерроризма. В проекте Концепции стратегии кибербезопасности Российской Федерации киберпространство определяется как «сфера деятельности в информационном пространстве, образованная совокупностью Интернета и других телекоммуникационных сетей и любых форм осуществляемой посредством их использования человеческой активности (личности, организации, государства)», а кибербезопасность – как «совокупность условий, при которых все составляющие киберпространства защищены от максимально возможного числа угроз и воздействий с нежелательными последствиями». В связи с этим большое значение приобретает проблема «культуры безопасного поведения в киберпространстве».

В соответствии со «Стратегией развития отрасли информационных технологий в Российской Федерации на 2014-2022 годы и на перспективу до 2025 года», утвержденной распоряжением Правительства Российской Федерации от 1 ноября 2013 г. № 2036-р, «Стратегией развития информационного общества в Российской Федерации», утвержденной Президентом Российской Федерации 7 февраля 2008 г. № Пр-212 и рядом других документов в числе многих других задач выделяются:

- обеспечение различных сфер экономики качественными информационными технологиями;
- обеспечение высокого уровня информационной безопасности государства, индустрии и граждан.

Безопасность в информационном обществе является одним из основных

направлений фундаментальных исследований в области информационных технологий.

Компьютерные технологии применяются при изучении практически всех школьных дисциплин уже с младших классов. Киберугрозы существуют везде, где применяются информационные технологии.

Государство считает необходимым расширение объема преподавания информационных технологий в общеобразовательных организациях. В качестве одной из организационных мер в обеспечении кибербезопасности определена разработка и внедрение в учебный процесс образовательных организаций разного уровня курса по информационной безопасности, включающего модули по обеспечению кибербезопасности, либо дополнение имеющихся курсов упомянутыми модулями. Школьная программа должна соответствовать этим целям, поэтому представляется актуальной реализация программы внеурочной деятельности «Информационная безопасность».

Задача программы «Информационная безопасность» - совершенствование школьного образования и подготовки в сфере информационных технологий, а также популяризация профессий, связанных с информационными технологиями. Цель изучения «Информационная безопасность» - дать общие представления о безопасности в информационном обществе и на этой основе сформировать понимание технологий информационной безопасности и умения применять правила кибербезопасности во всех сферах деятельности.

Воспитательная цель – формирование на качественно новом уровне культуры умственного труда и взаимодействия с окружающими, ответственного отношения к вопросам безопасности жизнедеятельности.

Цель программы – создание условий для формирования у учащихся цифровой культуры личности с необходимыми навыками и присущими ценностями, взглядами, ориентациями, установками, мотивами деятельности и поведения для обеспечения безопасной и развивающей жизнедеятельности учащегося в сети «Интернет».

Для достижения поставленной цели решаются следующие 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 и осуществления сетевых покупок;

- развить деловые и гражданские качества, такие как самостоятельность, ответственность, активность и аккуратность;

- сформировать потребности в самопознании и саморазвитии.

Воспитательные:

- воспитать культуру общения и поведения в сетевом пространстве;
- воспитать целеустремлённость личности;
- воспитать толерантную и культурную личность;
- воспитать правильный образ гражданина.

Программа по внеурочной деятельности «Информационная безопасность» структурирован по модульному принципу. Он включает в себя 7 модулей:

- общие сведения о безопасности ПК и Интернета
- техника безопасности и экология
- проблемы Интернет-зависимости
- методы обеспечения безопасности ПК и Интернета. Вирусы и

антивирусы

- мошеннические действия в Интернете. Киберпреступления
- сетевой этикет. Психология и сеть
- правовые аспекты защиты киберпространства

СОДЕРЖАНИЕ ОБУЧЕНИЯ

Модуль 1. Общие сведения о безопасности ПК и Интернета.

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.

Комплекс упражнений при работе за компьютером. Воздействие на зрение ЭЛТ, жидкокристаллических, светодиодных, монохромных мониторов.

Модуль 3. Проблемы Интернет-зависимости.

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

Модуль 4. Методы обеспечения безопасности ПК и Интернета. Вирусы и антивирусы.

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.

Модуль 5. Мошеннические действия в Интернете. Киберпреступления.

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. Предложения для «инвестирования» денег. Выигрыш в лотерею.

Модуль 6. Сетевой этикет. Психология и сеть

Психологическая обстановка в Интернете: гриффинг, кибербуллинг, кибер-

моббинг, троллинг, буллицид.

Модуль 7. Правовые аспекты защиты киберпространства .

Защита прав потребителей при использовании услуг Интернет. Защита прав потребителей услуг провайдера. Обобщение материала курса. Игра-квест «Знатоки кибербезопасности».

ПЛАНИРУЕМЫЕ РЕЗУЛЬТАТЫ ОСВОЕНИЯ ПРОГРАММЫ

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.

Метапредметные результаты. Регулятивные:

- 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:

- 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:

- 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 информацию с учетом этических и правовых норм;
- создавать информационные ресурсы разного типа и для разных аудиторий, соблюдать информационную гигиену и правила информационной безопасности.

Предметные. Обучающиеся научатся:

- 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.

Обучающиеся получат возможность научиться:

- приемам безопасной организации своего личного пространства данных, использованием индивидуальных накопителей данных, интернет-сервисов и т.п.
- основам соблюдения норм информационной этики и права;
- основам 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.

ТЕМАТИЧЕСКОЕ ПЛАНИРОВАНИЕ

№	Содержание	Количество часов
1.	Общие сведения о безопасности ПК и Интернета	5
2.	Техника безопасности и экология	2
3.	Проблемы интернетзависимости	3
4.	Методы обеспечения безопасности. Вирусы и антивирусы	16
5.	Мошеннические действия в Интернете. Киберпреступления	4
6.	Сетевой этикет. Психология и сеть.	1
7.	Правовые аспекты защиты киберпространства	3
ИТОГО		34

УЧЕБНО-МЕТОДИЧЕСКОЕ ОБЕСПЕЧЕНИЕ ОБРАЗОВАТЕЛЬНОГО ПРОЦЕССА

Учебно-методический комплекс программы «Логические и арифметические основы информатики» включает учебное пособие, программу, практические и контрольные работы, тесты.

Аппаратное обеспечение:

1. Моноблок и 12 ноутбуков.
2. Мультимедийный проектор, экран
3. Принтер, сканер
4. Видео – и DVD- проигрыватели
5. Интернет

ОБЯЗАТЕЛЬНЫЕ УЧЕБНЫЕ МАТЕРИАЛЫ ДЛЯ

УЧЕНИКА

1. Наместникова М.С. Информационная безопасность, или На расстоянии одного вируса. 7-9 классы. Внеурочная деятельность. – М.: Просвещение, 2019 – 80 с.

2. 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

МЕТОДИЧЕСКИЕ МАТЕРИАЛЫ ДЛЯ УЧИТЕЛЯ

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. Дети в информационном обществе <http://detionline.com/journal/about>

4. Ефимова Л.Л. Информационная безопасность детей. Российский и зарубежный опыт: Монография / Л.Л. Ефимова, С.А. Кочерга. – М.: ЮНИТИ-ДАНА, 2016 – 239 с.

5. Защита детей by Kaspersky // <https://kids.kaspersky.ru/>

6. Кузнецова А.В. Искусственный интеллект и информационная безопасность общества / А.В. Кузнецова, С.И. Самыгин, М.В. Радионов. – М.: Русайнс, 2017 – 64 с.

7. Наместникова М.С. Информационная безопасность, или На расстоянии одного вируса. 7-9 классы. Внеурочная деятельность. – М.: Просвещение, 2019 – 80 с.