*Государственное бюджетное общеобразовательное учреждение Самарской области средняя общеобразовательная школа № 2 с. Приволжье*
*муниципального района Приволжский Самарской области*

РАБОЧАЯ ПРОГРАММА

C=RU, O=ГБОУ СОШ №2 с.Приволжье, CN=Сергачева Л.Ю., E=school2_prv@samara.edu.ru
00f4a897f9467376cf
2022.06.02 15:59:17+04'00'

Проверено
Зам. Директор по УВР

_____
(подпись)
«02»_июня_ 2022г ___

Утверждаю
*Директор ГБОУ СОШ №2 с.Приволжье*

_____
(подпись)
«02»_июня_ 2022г

ТОЧКА РОСТА

**РАБОЧАЯ ПРОГРАММА**

Курса внеурочной деятельности:
Класс: 5-6 класс
Количество часов по учебному плану в 7-х классах 34 часов в год 1 час в неделю.
Учебное пособие для общеобразовательных организаций Наместникова М.С «Информационная безопасность, или расстоянии одного вируса» 7-9 класс : Москва «Просвещение» 2019.-79с. : ил.- (Внеурочная деятельность). – ISBN978-5-09-068966-3

Рассмотрена на заседании МО _____
(название методического объединения)
Протокол №_____от «_____»_____20____г.
Председатель МО _____
(ФИО) (подпись)

## Пояснительная записка.

Программа ориентирована на реализацию в Центре образования естественнонаучной и технологической направленностей «Точка роста», созданного на базе ГБОУ СОШ № 2 с. Приволжье с целью развития у обучающихся естественнонаучной, математической, информационной грамотности, формирования критического и креативного мышления, совершенствования навыков естественнонаучной и технологической направленности, а также для практической отработки учебного материала по учебным предметам «ОБЖ», «Технология», «Информатика».

На базе Центра «Точка роста» обеспечивается реализация образовательных программ естественнонаучной и технологической направленностей, разработанных в соответствии с требованиями законодательства в сфере образования и с учётом **МЕТОДИЧЕСКИХ МАТЕРИАЛОВ ФГАОУ ДПО «АКАДЕМИЯ МИНПРОСВЕЩЕНИЯ РОССИИ» ПО РЕАЛИЗАЦИИ ОБРАЗОВАТЕЛЬНОЙ ДЕЯТЕЛЬНОСТИ НА БАЗЕ ЦЕНТРА «ТОЧКА РОСТА»: Реализация образовательных программ по предмету "Информатика" с использованием оборудования центра "Точка Роста".**

Образовательная программа позволяет интегрировать реализуемые здесь подходы, структуру и содержание при организации обучения технологии в 7 классах, выстроенном на базе любого из доступных учебно- методических комплексов (УМК).

Использование оборудования Центра «Точка роста» позволяет создать условия:

- для расширения содержания школьного технологического образования;
- для повышения познавательной активности обучающихся в естественно-научной области;
- для развития личности ребенка в процессе обучения технологии, его способностей, формирования и удовлетворения социально значимых интересов и потребностей;

для работы с одарёнными школьниками, организации их развития в различных обла- стях образовательной и творческой деятельности. **Основная цель** изучения курса «Цифровая гигиена»:

 формирование навыков своевременного распознавания онлайн - рисков (технического, контентного, коммуникационного, потребительского характера и риска интернет -зависимости), повышения защищенности детей от информационных рисков и угроз;

**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 Интерне- том.

**Общая характеристика учебного курса**

Курс «Информационная безопасность» является важной составляющей работы с обучающимися, активно использующими различные сетевые формы общения (социальные сети, игры, пр.) с целью мотивации ответственного отношения обеспечению своейличной безопасности, безопасности своей семьи и своих друзей. Кроме того, реализация курса создаст условия для сокращения цифрового разрыва между поколениями и позволит родителям выступать в качестве экспертов, передающих опыт.

Данный курс предполагает организацию работы в соответствии с содержанием 2-х модулей,

предназначенных для обучающихся 7-9 классов и родителей обучающихся любого возраста соответственно.

**Модуль 1. «Информационная безопасность»**

Отбор тематики содержания курса осуществлен с учетом целей и задач ФГОС основного общего образования, возрастных особенностей и познавательных возможностей обучающихся 7-9 классов. Рекомендуется для реализации в рамках внеурочной деятельности обучающихся.

В преподавании модуля «Информационная безопасность» могут использоваться разнообразные форматы обучения: традиционный урок (коллективная и групповая формы работы), тренинги (в классической форме или по кейс- методу), дистанционное обучение (электронные курсы, видеоролики, почтовые рассылки, микрообучение ), смешанный формат.

Система учебных заданий должна создавать условия для формирования активной позиции

школьников в получении знаний и умений выявлять информационную угрозу, определять степень ее опасности, предвидеть последствия информационной угрозы и противостоять им и профилактики негативных тенденций в развитии информационной культуры учащихся, повышения защищенности детей от информационных рисков и угроз (составление памяток, анализ защищенности собственных аккаунтов в социальных сетях и электронных сервисах, практические работы и т.д.).

**Место учебного курса (Модуль 1) в учебном плане**

Программа учебного курса (Модуль 1) рассчитана на 34 учебных часа, из них 22часа – учебных занятий, 9 часов – подготовка и защита учебных проектов, 3 часа –повторение. На изучение модуля 1 «Информационная безопасность» отводится по1 часу в неделю в 7, 8 или 9 классах. Учебные занятия по программе могут быть реализованы в различных вариантах:

1. в течение одного учебного года в 7, 8 или 9 классах. В этом случае программа рассчитана на 34 учебных часа;
2. по одномуразделу последовательно в 7, 8 и 9 классах;
3. произвольно распределены учителем в зависимости от интереса и готовности школьников.

**Характеристика личностных, метапредметных и предметных результатов освоенияучебного курса (Модуль 1)**

***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 конечныйрезультат;
- ставить цель деятельности на основе определенной проблемы и существующихвозможностей;
- выбирать из предложенных вариантов и самостоятельно искать средства/ресурсы длярешения 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 гигиенуи 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.

**Содержание программы учебного курса (Модуль 1).**

Содержание программы учебного курса (Модуль 1) соответствует темам примерной основной образовательной программы основного общего образования (ПООП ООО) по учебнымпредметам «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 (Модуля 1) завершается выполнением проектной работы по одной из тем, предложенных на выбор учащихся и/или проверочного теста.

За счет часов, предусмотренных для повторения материала (4 часа), возможно проведение занятий для учащихся 4-6 классов. Эти занятия в качестве волонтерской практики могут быть проведены учащимися, освоившими программу. Для проведения занятий могут быть использованы презентации, проекты, памятки, онлайн занятия, подготовленные в ходе выполнения учебных заданий по основным темам курса.

## Содержание учебного курса 7 класс (Модуль 1).

### Раздел 1. «Безопасность общения»

**Тема 1. Общение в социальных сетях и мессенджерах. 1 час.**

Социальная сеть. История социальных сетей. Мессенджеры. Назначение социальных сетей и мессенджеров. Пользовательский контент.

**Тема 2. С кем безопасно общаться в интернете. 1 час.**

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

**Тема 3. Пароли для аккаунтов социальных сетей. 1 час.**

Сложные пароли. Онлайн генераторы паролей. Правила хранения паролей. Использование функции браузера по запоминанию паролей.

**Тема 4. Безопасный вход в аккаунты. 1 час.**

Виды аутентификации. Настройки безопасности аккаунта. Работа на чужом компьютере сточки зрения безопасности личного аккаунта.

**Тема 5. Настройки конфиденциальности в социальных сетях. 1 час.**

Настройки приватности и конфиденциальности в разных социальных сетях. Приватность и конфиденциальность в мессенджерах.

**Тема 6. Публикация информации в социальных сетях. 1 час.**

Персональные данные. Публикация личной информации.

**Тема 7. Кибербуллинг. 1 час.**

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

**Тема 8. Публичные аккаунты. 1 час.**

Настройки приватности публичных страниц. Правила ведения публичных страниц. Овершеринг.

**Тема 9. Фишинг. 2 часа.**

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. 3 часа. 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 кодовна устройствах. Действия при обнаружении вредоносных кодов на устройствах.

**Тема 3. Методы защиты от вредоносных программ. 2 час.**

Способы защиты устройств от вредоносного кода. Антивирусные про- граммы 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. 3 часа.[4]Раздел 3 «Безопасность информации»**

**Тема 1. Социальная инженерия: распознать и избежать.**

Приемы социальной инженерии. Правила безопасности при виртуальных контактах.

**Тема 2. Ложная информация в Интернете.**

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

**Тема 3. Безопасность при использовании платежных карт в Интернете.**

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

**Тема 4. Беспроводная технология связи.**

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

**Тема 5. Резервное копирование данных.**

Безопасность личной информации. Создание резервных копий на различных устройствах.

**Тема 6. Основы государственной политики в области формирования культуры информационной безопасности.**

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.**

**Повторение. Волонтерская практика.**

**Тематическое планирование учебного курса 7 класс (Модуль 1).**

| № п/п | Тема | Кол-во часов | Результат *(в рамках конкретной указанной темы)* | Оборудование центра «Точка Роста» |
|---|---|---|---|---|
| **Тема 1. «Безопасность общения»** | | | | |
| 1 | Общение в социальных сетях и мессенджерах | 1 | Выполняет базовые операциипри использовании мессенджеров и социальных сетей. Создает свой образ в сети Интернет. Изучает историю и социальную значимость личных аккаунтов в сети Интернет. | Ноутбуки мобильного класса, интерактивный комплекс |
| 2 | С кем безопасно общаться винтернете | 1 | Руководствуется в общении социальными ценностями и установками коллектива и общества в целом. Изучает правила сетевого общения. | Ноутбуки мобильного класса, интерактивный комплекс |
| 3 | Пароли для аккаунтов социальных сетей | 1 | Ноутбуки мобильного класса, интерактивный комплекс | Ноутбуки мобильного класса, интерактивный комплекс |
| 4 | Безопасный вход в Аккаунты | 1 | Объясняет причины использования безопасного входа при работе на чужом устройстве. Демонстрирует устойчивый навык безопасного входа. | Ноутбуки мобильного класса, интерактивный комплекс |
| 5 | Настройки конфиденциальности всоциальных сетях | 1 | Раскрывает причины установки закрытого профиля. Меняет основные настройки приватности в личном профиле. | Ноутбуки мобильного класса, интерактивный комплекс |
| 6 | Публикация информации всоциальных сетях | 1 | Осуществляет поиск и использует информацию, необходимую для выполнения поставленных задач. | Ноутбуки мобильного класса, интерактивный комплекс |

| | | | | |
|---|---|---|---|---|
| 7 | Кибербуллинг | 1 | Реагирует на опасные ситуации, распознает провокации и попытки манипуляции со стороны виртуальных собеседников. | Ноутбуки мобильного класса, интерактивный комплекс |
| 8 | Публичные аккаунты | 1 | Решает эк сперимен тальные задачи. Самостоятельно создает источники информации разного типа и для разных аудиторий, соблюдая правила информационной безопасности. | Ноутбуки мобильного класса, интерактивный комплекс |
| 9 | Фишинг | 2 | Анализ проблем ных ситуаций .Разработка кейсов с примерами | Ноутбуки мобильного класса, интерактивный комплекс |

| | | | | |
|---|---|---|---|---|
| | | | из личной жизни/жизни знакомых. Разработка и распространение чек- листа (памятки) по противодействию фишингу. | |
| 10 | Выполнение и защита индивидуальных и групповых проектов | 3 | Самостоятельная работа. | Ноутбуки мобильного класса, интерактивный комплекс |
| **Тема 2. «Безопасность устройств»** | | | | |
| 1 | Что такое вредоносный код | 1 | Соблюдает технику безопасности при эксплуатации компьютерных систем. Использует инструментальные программные средства и сервисыадекватно задаче. | Ноутбуки мобильного класса, интерактивный комплекс |
| 2 | Распространение вредоносного кода | 1 | Выявляет и анализирует (при помощи чек-листа) возможные угрозы информационной безопасности объектов. | Ноутбуки мобильного класса, интерактивный комплекс |
| 3 | Методы защиты от вредоносных программ | 2 | Изучает виды антивирусных программ и правила их установки. | Ноутбуки мобильного класса, интерактивный комплекс |
| | | | | |
| 4 | Распространение вредоносного кода для мобильных устройств | 1 | Разрабатывает презентацию, инструкциюпо обнаружению, алгоритм установки | Ноутбуки мобильного класса, интерактивный комплекс |

| | | | | |
|---|---|---|---|---|
| | | | приложений на мобильные устройства для учащихся более младшего возраста. | |
| 5. | Выполнение и защита индивидуальных и групповых проектов | 3 | Умеет работать индивидуально и вгруппе. Принимает позицию собеседника, понимая позицию другого, различает в его речи: мнение (точку зрения), доказательство (аргументы), факты; гипотезы, аксиомы, теории. | Ноутбуки мобильного класса, интерактивный комплекс |
| **Тема 3 «Безопасность информации»** | | | | |
| 1 | Социальная инженерия: распознать и избежать | 1 | Находит нужную информацию в базахданных, составляя запросы на поиск. Систематизирует получаемую информацию в процессе поиска. | Ноутбуки мобильного класса, интерактивный комплекс |
| 2 | Ложная информация в Интернете | 1 | Определяет возможные источники необходимых сведений, осуществляет поиск информации. Отбирает и сравнивает материал по нескольким источникам. | Ноутбуки мобильного класса, интерактивный комплекс |

| | | | | |
|---|---|---|---|---|
| | | | Анализирует и оценивает достоверность информации. | |
| 3 | Безопасность при использовании платежных карт в Интернете | 1 | Приводит примеры рисков, связанных с совершением онлайн покупок (умеет определитьисточник риска). Разрабатывает возможные варианты решения ситуаций, связанных срисками использования платежных карт в Интернете. | Ноутбуки мобильного класса, интерактивный комплекс |
| 4 | Беспроводная технология связи | 1 | Используя различную информацию, определяет понятия. Изучает особенностии стиль ведения личных и публичных аккаунтов. | Ноутбуки мобильного класса, интерактивный комплекс |
| 5 | Резервное копирование данных | 1 | Создает резервные копии. | Ноутбуки мобильного класса, интерактивный комплекс |
| 6 | Основы государственной политики в области формирования культуры информационной безопасности | 2 | Умеет привести выдержки из законодательстваРФ, обеспечивающего конституционное право на поиск, получение и распространение информации, отраж | Ноутбуки мобильного класса, интерактивный комплекс |

| | | | | |
|---|---|---|---|---|
| | | | ающего правовые аспекты<br><br>защиты киберпространства. | |
| 7 | Выполнение и защита индивидуальных и групповых проектов | 3 | | |
| 8 | Повторение, волонтерская практика, резерв | 3 | | |
| | Итого | 34 | | |

**Список источников:**


1. Бабаш А.В. Информационная безопасность: Лабораторный практи- кум / 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 за- кон, 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
5. Ефимова Л.Л. Информационная безопасность детей. Российский и зарубежный опыт: Монография / Л.Л. Ефимова, С.А. Кочерга. – М.: ЮНИТИ-ДАНА, 2016. – 239 с.
6. Запечников С.В. Информационная безопасность открытых систем. В2-х т. Т.2 – Средства защиты в сетях / С.В. Запечников, Н.Г. Милославская, А.И. Толстой, Д.В. Ушаков. – М.: ГЛТ, 2018. – 558 с.
7. Защита детей by Kaspersky // https://kids.kaspersky.ru/
8. Кузнецова А.В. Искусственный интеллект и информационная без- опасность общества / А.В. Кузнецова, С.И. Самыгин, М.В. Радионов. – М.: Ру-сайнс, 2017. – 64 с.
9. Наместникова М.С. Информационная безопасность, или На расстоя-нии одного вируса. 7-9 классы. Внеурочная деятельность. – М.: Просвещение,2019. – 80 с.
10. Основы кибербезопасности. // https://www.xn--d1abkefqip0a2f.xn--p1ai/index.php/glava-1-osnovy-kiberbezopasnosti-tseli-i-zadachi-kursa
11. Стрельцов А.А. Правовое обеспечение информационной безопасно-сти России: теоретические и методологические основы. – Минск, 2005. – 304 с.
12. Сусоров И.А. Перспективные технологии обеспечения кибербез- опасности // Студенческий: электрон. научн. журн. 2019. № 22(66)
13. Цифровая компетентность подростков и родителей. Результаты все-российского исследования / Г.У. Солдатова, Т.А. Нестик, Е.И. Рассказова, Е.Ю. Зотова. – М.: Фонд Развития Интернет, 2013. – 144 с.