




муниципальное бюджетное общеобразовательное учреждение
«Школа № 137 имени М.П. Агибалова» городского округа Самара

<p>УТВЕРЖДЕНО</p> <p>ДИРЕКТОР</p>  <p>Марков О.Е.</p> <p>Приказ № 197-од от «30» августа 2021г.</p>	<p>СОГЛАСОВАНО</p> <p>Зам. директора по УВР</p>  <p>Кочеткова О.В.</p> <p>« 30 » августа 2021г.</p>	<p>РАССМОТРЕНО</p> <p>на заседании ШМО учителей естественно-математического цикла</p> <p>Председатель ШМО</p>  <p>Дерябина О.А.</p> <p>Протокол № 1 от «30» августа 2021г.</p>
--	--	---

РАБОЧАЯ ПРОГРАММА

курса внеурочной деятельности «Информационная безопасность»
для обучающихся 7-9 классов

форма организации: факультатив
Направление: общекультурное
Срок реализации: 3 года

Разработана
Барановым И.В.,
учитель информатики

Самара, 2021

Пояснительная записка

Программа курса внеурочной деятельности «Информационная безопасность» для 7-9 классов разработана в соответствии с требованиями Федерального государственного образовательного стандарта основного общего образования (ФГОС ООО) и Основной образовательной программы основного общего образования (ООП ООО) МБОУ Школы №137 г.о. Самара.

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

Отбор тематики содержания курса осуществлен с учетом возрастных особенностей и познавательных возможностей обучающихся 7-9 классов.

Система учебных заданий создает 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 обучающихся, 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.).

В преподавании курса внеурочной деятельности «Информационная безопасность» 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, микрообучение), смешанный формат.

Место учебного курса в учебном плане

Программа курса внеурочной деятельности рассчитана на 34 учебных часа в год (по 1 часу в неделю), из них 22 часа - учебных занятий, 9 часов - подготовка и защита учебных проектов, 3 часа - повторение. Учебные занятия по программе реализуются в течение одного учебного года в 7, 8 и 9 классах.

Цель и задачи изучения

Основными целями изучения курса внеурочной деятельности «Информационная безопасность» являются:

- обеспечение условий для профилактики негативных тенденций в информационной культуре обучающихся, 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.

Планируемые результаты освоения курса внеурочной деятельности

Личностные.

Выпускник научится:

- осознанному, уважительному и доброжелательному отношению к окружающим людям в реальном и виртуальном мире, их позициям, взглядам, готовности вести диалог с другими людьми, обоснованно осуществлять выбор виртуальных собеседников;

- готовности и способности к осознанному выбору и построению дальнейшей индивидуальной траектории образования на базе ориентировки в мире профессий и профессиональных предпочтений, с учетом устойчивых познавательных интересов; - освоенности социальных норм, правилам поведения, ролей и форм социальной жизни в группах и сообществах; *Выпускник получит возможность:*

- сформировать понимание ценности безопасного образа жизни; отработать правила индивидуального и коллективного безопасного поведения в информационно-телекоммуникационной среде.

Метапредметные.

Регулятивные универсальные учебные действия.

Выпускник научится:

- 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;

Выпускник получит возможность:

- 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.

Выпускник научится:

- 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; *Выпускник получит возможность:*
- 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.

Выпускник научится:

- 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; *Выпускник получит возможность:*

- 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.

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.

Воспитательные результаты:

Первый уровень (приобретение школьником социальных знаний) - приобретение обучающимися знаний о правилах пользования компьютером; о способах нахождения и обработки информации и защите своих персональных данных в социальных сетях.

Второй уровень (получение школьником опыта переживания и позитивного отношения к базовым ценностям общества) - школьник может приобрести опыт публичного выступления, проведения опросов обучающихся школы, родителей, учителей; опыт общения, чувства ответственности за других людей, опыт управления другими людьми, развитие ценностных отношений к своему здоровью и внутреннему миру.

Учебно-тематический план

№	Название раздела	Часы аудиторных занятий	Часы практических занятий (не менее 50%)	Общее кол-во часов
1.	Безопасность общения	7	6	13
2.	Безопасность устройств	3	4	7
3.	Безопасность информации	7	7	14
	ИТОГО	17 (50%)	17 (50%)	34 (100%)

Содержание программы

Содержание программы курса внеурочной деятельности соответствует темам примерной основной образовательной программы основного общего образования (ПООП ООО) по учебным предметам «Информатика», 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 курса 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 обучающихся 4-6 классов. Эти занятия в качестве волонтерской практики могут быть проведены обучающимися, освоившими программу. Для проведения занятий могут быть использованы презентации, проекты, памятки, он-лайн занятия, подготовленные в ходе выполнения учебных заданий по основным темам курса.

№	Название темы	Краткое содержание темы	Формы организации образовательного процесса	Сроки
----------	----------------------	--------------------------------	--	--------------

Безопасность общения				
1	Общение в социальных сетях и мессенджерах	Социальная сеть. История социальных сетей. Мессенджеры. Назначение социальных сетей и мессенджеров. Пользовательский контент.	Беседа	Сентябрь, 1 неделя
2	С кем безопасно общаться в интернете	Персональные данные как основной капитал личного пространства в цифровом мире. Правила добавления друзей в социальных сетях. Профиль пользователя. Анонимные социальные сети.	Объяснение	Сентябрь, 2 неделя
3	Пароли для аккаунтов социальных сетей	Сложные пароли. Онлайн генераторы паролей. Правила хранения паролей. Использование функции браузера по запоминанию паролей.	Видеоролик	Сентябрь, 3 неделя
4	Безопасный вход в аккаунты	Виды аутентификации. Настройки безопасности аккаунта. Работа на чужом компьютере с точки зрения безопасности личного аккаунта.	Беседа	Сентябрь, 4 неделя
5	Настройки конфиденциальности в социальных сетях	Настройки приватности и конфиденциальности в разных социальных сетях. Приватность и конфиденциальность в мессенджерах.	Практическая работа	Октябрь, 5 неделя
6	Публикация информации в социальных сетях	Персональные данные. Публикация личной информации.	Объяснение	Октябрь, 6 неделя
7	Кибербуллинг	Определение кибербуллинга. Возможные причины кибербуллинга и как его избежать? Как не стать жертвой кибербуллинга. Как помочь жертве кибербуллинга.	Видеоролик	Октябрь, 7 неделя
8	Публичные аккаунты	Настройки приватности публичных страниц. Правила ведения публичных страниц. Овершеринг.	Беседа	Октябрь, 8 неделя
9	Публичные аккаунты	Настройки приватности публичных страниц. Правила ведения публичных страниц. Овершеринг.	Видеоролик	Ноябрь, 9 неделя
10	Фишинг	Фишинг как мошеннический прием. Популярные варианты распространения фишинга. Отличие настоящих и фишинговых сайтов. Как защититься от фишеров в социальных сетях и мессенджерах.	Видеоролик	Ноябрь, 10 неделя
11-13	Работа над индивидуальными проектами	Выполнение и защита индивидуальных и групповых проектов	Групповая	Ноябрь, 11,12 недели Декабрь, 13 неделя

№	Название темы	Краткое содержание темы	Формы организации образовательного процесса	Сроки
Безопасность устройств				
14	Что такое вредоносный код	Виды вредоносных кодов. Возможности и деструктивные функции вредоносных кодов.	Беседа	Декабрь, 14 неделя
15	Распространение вредоносного кода	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.	Обсуждение	Декабрь, 15 неделя
16-17	Методы защиты от вредоносных программ	Способы защиты устройств от вредоносного кода. Антивирусные программы и их характеристики. Правила защиты от вредоносных кодов.	Объяснение	Декабрь, 16 неделя Январь, 17 неделя
18	Распространение вредоносного кода для мобильных устройств	Расширение вредоносных кодов для мобильных устройств. Правила безопасности при установке приложений на мобильные устройства.	Видеоролик	Январь, 18 неделя
19-21	Работа над индивидуальными проектами	Выполнение и защита индивидуальных и групповых проектов	Групповая	Январь, 19 неделя Февраль, 20, 21 недели
Безопасность информации				
22	Социальная инженерия: распознать и избежать	Приемы социальной инженерии. Правила безопасности при виртуальных контактах.	Беседа	Февраль, 22 неделя
23	Ложная информация в Интернете	Цифровое пространство как площадка самопрезентации, экспериментирования и освоения различных социальных ролей. Фейковые новости. Поддельные страницы.	Видеоролик	Февраль, 23 неделя
24	Безопасность при использовании платежных карт в Интернете	Транзакции и связанные с ними риски. Правила совершения он-лайн покупок. Безопасность банковских сервисов.	Видеоролик	Март, 24 неделя
25	Беспроводная технология связи	Уязвимость Wi-Fi-соединений. Публичные и непубличные сети. Правила работы в публичных сетях.	Практикум	Март, 25 неделя

26	Резервное копирование данных	Безопасность личной информации. Создание резервных копий на различных устройствах.	Практикум	Март, 26 неделя
27-28	Основы государственной политики в области формирования культуры	Доктрина национальной информационной безопасности. Обеспечение свободы и равенства доступа к информации и знаниям. Основные направления государственной политики	Беседа	Апрель, 27,28 недели
№	Название темы	Краткое содержание темы	Формы организации образовательного процесса	Сроки
	информационной безопасности	в области формирования культуры информационной безопасности.		
29-30	Работа над индивидуальными проектами	Выполнение и защита индивидуальных и групповых проектов	Групповая	Апрель, 29,30 недели
31-34	Повторение. Волонтерская практика	Проведение занятий для обучающихся 4-6 классов.	Групповая	Май, 31-34 недели

Формы диагностики и подведения итогов

В итоге изучения материала учащиеся пишут рефераты, выступающие в качестве итоговой практической работы. Контроль за изученным материалом осуществляется в форме тематических рисунков, кроссвордов, презентаций, тестов, рефератов, устных ответов, собеседования. Текущий контроль за усвоением материала осуществляется на каждом занятии посредством мини-опроса и выполнения практических заданий.

Литература для учителя:

1. Попов В. Б. Основы информационных и телекоммуникационных технологий. Основы информационной безопасности: Учебное пособие. - М.: Финансы и статистика, 2005.
2. Морозов Н.П., Чернокнижный С.Б. Защита деловой информации для всех. - . СПб.: ИД «ВЕСЬ», 2003.
3. Леонтьев Б.К. Если «зависла» MicrosoftWindowsXP ... /Борис Леонтьев. - М.: ЗАО «Новый издательский дом», 2005.
4. ЛеонтьевБ. К. Microsoft Windows XP SP3. Скрытые возможности. - М.: ИТ Пресс, 2006.
5. Касперски К. Записки исследователя компьютерных вирусов. - СПб.: Питер, 2006.

6. Майнулов В.Г. Энциклопедия учителя информатики: MicrosoftWindowsXP в вопросах и ответах. – М.: Образование и Информатика, 2005. – Библиотека журнала «Информатика и образование».
7. Материалы газеты «Информатика».
8. Интернет-ресурсы

Литература для обучающихся:

1. Попов В. Б. Основы информационных и телекоммуникационных технологий. Основы информационной безопасности: Учебное пособие. – М.: Финансы и статистика, 2005.
2. Касперский К. Записки исследователя компьютерных вирусов. - СПб.: Питер, 2006.
3. Майнулов В.Г. Энциклопедия учителя информатики: MicrosoftWindows в вопросах и ответах. – М.: Образование и Информатика, 2005. – Библиотека журнала «Информатика и образование».
4. Материалы газеты «Информатика».
5. Интернет-ресурсы

Темы проектов

№	Тема	Предполагаемый продукт	Практическая значимость
1.	Вирусы и борьба с ними.	Памятка	Разработка конкретных рекомендаций по защите в интернете.
2.	История компьютерного пиратства и систем защиты информации.	Исследовательская работа	Знакомство с историей.
3.	Телеконференция системы Usenet.	Исследовательская работа	Обзор системы.
4.	Мир без Интернета	Исследовательская работа	Высказывание гипотезы и её обоснование.
5.	Популярные антивирусные программные средства.	Буклет	Разработка конкретных рекомендаций по выбору антивирусных программ.
6.	Правила этикета при работе с компьютерной сетью.	Исследовательская работа	Разработка конкретных рекомендаций по правилам общения в интернете.
7.	Социальные сети в жизни обучающихся нашей школы.	Исследовательская работа	Результаты могут использоваться обучающимися, учителями, родителями.
8.	Спам и защита от него.	Исследовательская работа	Разработка конкретных рекомендаций по защите в интернете.
9.	Техника безопасности при работе с ПК 30 лет назад и сейчас.	Исследовательская работа	Сравнение систем защиты «сегодня» и «вчера».
10.	Шифрование информации.	Исследовательская работа	Разработка конкретных рекомендаций по шифрованию.