муниципальное бюджетное общеобразовательное учреждение
«Школа № 144 имени Маршала Советского Союза Д. Ф. Устинова»
городского округа Самара

РАССМОТРЕНО	ПРОВЕРЕНО	УТВЕРЖДЕНО
на заседании МО учителей гуманитарного цикла Протокол №1 от «27» августа 2021 г. Председатель МО _____/Куляева Е.О./	Заместитель директора по УВР _____/ Куляева Е.О. / «28» августа 2021 г.	Директор МБОУ Школы № 144 г.о.Самара _____/ Волохова Т.В./ «30» августа 2021г. Приказ №90 от «30» августа 2021 г.

РАБОЧАЯ ПРОГРАММА
по информационной безопасности

уровень обучения: основное общее образование
Составители: учителя истории и обществознания: Куляева Е.О.

1. Пояснительная записка

Программа курса «Информационная безопасность» адресована учащимся 8 класса и учитывает требования, выдвигаемые федеральным государственным образовательным стандартом основного общего образования к предметным (образовательные области «Математика и информатика», «Физическая культура и основы безопасности жизнедеятельности»), метапредметным и личностным результатам.

Рабочая программа разработана на основе:

- Федеральный Закон от 29.12.2012 № 273-ФЗ «Об образовании в Российской Федерации» (ред. от 06.03.2019).
- Постановление Главного Государственного врача Российской Федерации от 30 июня 2020 г. N 16 Санитарно-эпидемиологические правила СП 3.1/2.4.3598-20 "Санитарно-эпидемиологические требования к устройству, содержанию и организации работы образовательных организаций и других объектов социальной инфраструктуры для детей и молодежи в условиях распространения новой коронавирусной инфекции (COVID-19)".
- Постановление Главного Государственного врача Российской Федерации от 28 сентября 2020 г. № 28 Об утверждении санитарных правил СП 2.4.3648-20 "Санитарно-эпидемиологические требования к организациям воспитания и обучения, отдыха и оздоровления детей и молодежи".
- Федеральный перечень учебников, утвержденный приказом Министерства просвещения Российской Федерации от 20.05.2020 № 254 (с изменениями от 23.12.2020 № 766);
- Федеральный перечень учебников, утвержденный приказом Минпросвещения России от 28.12.2018 № 345 (учебники, приобретенные из федерального перечня 2018 года до вступления в силу данного приказа, образовательные организации вправе использовать в течение пяти лет);
- Федеральный перечень учебников, утвержденный приказом Минобрнауки России от 31.03.2014 № 253 (в соответствии с приказом Минпросвещения России от 28.12.2018 № 345 учебники, приобретенные из федерального перечня 2014 года до вступления в силу данного приказа, образовательные организации вправе использовать в течение трех лет)
- Федеральный государственный образовательный стандарт основного общего образования, утвержденный приказом Министерства образования и науки Российской Федерации от 17.12.2010 № 1897 (в ред. приказа № 1577 от 31.12.15).
- Письмо Минобрнауки России от 18.08.2017 № 09-1672 «О направлении Методических рекомендаций по уточнению понятия и содержания внеурочной деятельности в рамках реализации основных

общеобразовательных программ, в том числе в части проектной деятельности»;

- Приказ Министерства просвещения Российской Федерации от 22.03.2021 № 115 "Об утверждении Порядка организации и осуществления образовательной деятельности по основным общеобразовательным программам - образовательным программам начального общего, основного общего и среднего общего образования".
- Письмо Рособрнадзора от 20.06.2018 N 05-192 «О реализации прав на изучение родных языков из числа языков народов РФ в общеобразовательных организациях»
- Приказ министерства образования и науки Самарской области от 04.09.2014 № 276-ОД «Об утверждении Порядка регламентации и оформления отношений государственной и муниципальной образовательной организации, и родителей (законных представителей) обучающихся, нуждающихся в длительном лечении, а также детей-инвалидов, осваивающих основные общеобразовательные программы на дому, в Самарской области». (с изм от 10 августа 2016 г. N 259-од)
- Письмо министерства образования и науки Самарской области от 23.08.2016 № 815-ТУ. «Об организации обучения на дому по основным общеобразовательным программам обучающихся, нуждающихся в длительном лечении, а также детей-инвалидов».
- Письмо Министерства образования и науки Самарской области от 17.02.2016 № МО-16-09-01/173-ту «О внеурочной деятельности».
- ООП ООО МБОУ Школы № 144 г.о. Самара.
- АООП ООО МБОУ Школы №144 г.о.Самара
- Рабочая программа воспитания МБОУ Школы №144 г.о.Самара
- Учебный план МБОУ Школы №144 г.о. Самара
- Календарного учебного графика МБОУ Школы №144 г.о.Самара

Основными целями изучения курса «Информационная безопасность» 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.

Место учебного курса в учебном плане

Программа учебного курса (Модуль 1) рассчитана на 34 учебных часа, из них 22 часа – учебных занятий, 9 часов – подготовка и защита учебных проектов, 3 часа – повторение. На изучение модуля 1 «Информационная безопасность» отводится по 1 часу в неделю 8 классе.

2. Планируемые результаты изучения учебного предмета

Практическая реализация рабочей программы воспитания осуществляется в рамках **модуля 3.4. «Школьный урок».**

Реализация школьными педагогами воспитательного потенциала урока предполагает следующее:

- установление доверительных отношений между учителем и его учениками, способствующих позитивному восприятию учащимися требований и просьб учителя, привлечению их внимания к обсуждаемой на уроке информации, активизации их познавательной деятельности ***(Изучение разделов: «Безопасность общения», «Безопасность устройств», «Безопасность информации»);***
- побуждение школьников соблюдать на уроке общепринятые нормы поведения, правила общения со старшими (учителями) и сверстниками (школьниками), принципы учебной дисциплины и самоорганизации ***(Изучение разделов: «Безопасность общения», «Безопасность устройств», «Безопасность информации»);***
- привлечение внимания школьников к ценностному аспекту изучаемых на уроках явлений, организация их работы с получаемой на уроке социально значимой информацией – инициирование ее обсуждения, высказывания учащимися своего мнения по ее поводу, выработки своего к ней отношения

(Изучение разделов: «Безопасность общения», «Безопасность устройств», «Безопасность информации»);

- использование воспитательных возможностей содержания учебного предмета через демонстрацию детям примеров ответственного, гражданского поведения, проявления человеколюбия и добросердечности, через подбор соответствующих текстов для чтения, задач для решения, проблемных ситуаций для обсуждения в классе ***(Изучение разделов: «Безопасность общения», «Безопасность устройств», «Безопасность информации»);***
- применение на уроке интерактивных форм работы учащихся: интеллектуальных игр, стимулирующих познавательную мотивацию школьников; дискуссий, которые дают учащимся возможность приобрести опыт ведения конструктивного диалога; групповой работы или работы в парах, которые учат школьников командной работе и взаимодействию с другими детьми ***(Изучение разделов: «Безопасность общения», «Безопасность устройств», «Безопасность информации»);***
- включение в урок игровых процедур, которые помогают поддержать мотивацию детей к получению знаний, налаживанию позитивных межличностных отношений в классе, помогают установлению доброжелательной атмосферы во время урока ***(Изучение разделов: «Безопасность общения», «Безопасность устройств», «Безопасность информации»);***
- организация шефства мотивированных и эрудированных учащихся над их неуспевающими одноклассниками, дающего школьникам социально значимый опыт сотрудничества и взаимной помощи ***(Изучение разделов: «Безопасность общения», «Безопасность устройств», «Безопасность информации»);***
- инициирование и поддержка исследовательской деятельности школьников в рамках реализации ими индивидуальных и групповых исследовательских проектов, что даст школьникам возможность приобрести навык самостоятельного решения теоретической проблемы, навык генерирования и оформления собственных идей, навык уважительного отношения к чужим идеям, оформленным в работах других исследователей, навык публичного выступления перед аудиторией, аргументирования и отстаивания своей точки зрения ***(Изучение разделов: «Безопасность общения», «Безопасность устройств», «Безопасность информации»).***

Личностные результаты:

-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 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.

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 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 получит возможность научиться:
-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.

3. Содержание программы учебного курса.

Содержание программы учебного курса соответствует темам примерной основной образовательной программы основного общего образования (ПООП ООО) по учебным предметам «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 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.

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 с точки 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 кодов на устройствах. Действия при обнаружении вредоносных кодов на устройствах.

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

Способы защиты устройств от вредоносного кода. Антивирусные программы 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. 1 час.

Приемы социальной инженерии. Правила безопасности при виртуальных контактах.

Тема 2. Ложная информация в Интернете. 1 час.

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

Тема 3. Безопасность при использовании платежных карт в Интернете. 1 час.

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

Тема 4. Беспроводная технология связи. 1 час.

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

Тема 5. Резервное копирование данных. 1 час.

Безопасность личной информации. Создание резервных копий на различных устройствах.

Тема 6. Основы государственной политики в области формирования культуры информационной безопасности. 2 час.

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. 3 часа.5

Повторение. Волонтерская практика. 3 часа.

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. В 2-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.

Тематическое планирование 8 класс (34ч.)

№	Тема	Кол-во часов	РПВ
Тема 1. «Безопасность общения»			
1	Общение в социальных сетях и мессенджерах	1	В.М.3.4.
2	С кем безопасно общаться в интернете	1	В.М.3.4.
3	Пароли для аккаунтов социальных сетей	1	В.М.3.4.
4	Безопасный вход в аккаунты	1	В.М.3.4.
5	Настройки конфиденциальности в социальных сетях	1	В.М.3.4.
6	Публикация информации в социальных сетях	1	В.М.3.4.
7	Кибербуллинг	1	В.М.3.4.
8	Публичные аккаунты	1	В.М.3.4.
9	Фишинг	2	В.М.3.4.
10	Выполнение и защита индивидуальных и групповых проектов	3	В.М.3.4.
Тема 2. «Безопасность устройств»			
11	Что такое вредоносный код	1	В.М.3.4.
12	Распространение вредоносного кода	1	В.М.3.4.
13	Методы защиты от вредоносных программ	2	В.М.3.4.
14	Распространение вредоносного кода для мобильных устройств	1	В.М.3.4.
15	Выполнение и защита индивидуальных и групповых проектов	3	В.М.3.4.
Тема 3 «Безопасность информации»			
16	Социальная инженерия: распознать и избежать	1	В.М.3.4.
17	Ложная информация в Интернете	1	В.М.3.4.
18	Безопасность при использовании платежных карт в Интернете	1	В.М.3.4.
19	Беспроводная технология связи	1	В.М.3.4.
20	Резервное копирование данных	1	В.М.3.4.

21	Основы государственной политики в области формирования культуры информационной безопасности	2	В.М.3.4.
22	Выполнение и защита индивидуальных и групповых проектов	3	В.М.3.4.
23	Повторение, волонтерская практика, резерв	3	В.М.3.4.
Итого		34	