муниципальное бюджетное общеобразовательное учреждение
«Школа № 98» городского округа Самара

РАССМОТРЕНО	СОГЛАСОВАНО	УТВЕРЖДАЮ
На заседании МО учителей гуманитарного цикла	Зам. директора по ВР	Директор МБОУ Школа № 98
Протокол № 1 от 28.08.20	Орлянская Е.А.	Юсупова А. Э.
Руководитель МО Луханова О.В.	«28» 08 20 20 г.	Приказ № 880 от 01.09.2020

Рабочая программа внеурочной деятельности

«Информационная безопасность»

для 8 класса

направление: общеинтеллектуальное

Составитель:
Романова О.В.
учитель иностранного
языка

Самара

Пояснительная записка

При составлении программы курса внеурочной деятельности «Информационная безопасность» автором использованы следующие нормативно-правовые документы:

- Федеральный закон от 29.12.2012 №273-ФЗ «Об образовании в Российской Федерации»;
- Постановление Главного государственного врача РФ от 29.12.2010г. №189 «Об утверждении СанПиН 2.4.2.2821-10 «Санитарно-эпидемиологические требования к условиям и организации обучения в общеобразовательных учреждениях»;
- Федеральный государственный образовательный стандарт основного общего образования, утвержденный приказом Министерства образования и науки Российской Федерации от 17.12.2010г. № 1897 (п.18.2.2);
- Приказ № 1577 от 31 декабря 2015 г. Минобрнауки России «О внесении изменений в федеральный государственный образовательный стандарт основного общего образования, утвержденный приказом Министерства образования и науки российской Федерации от 17 декабря 2010 г. №1897»;
- Информационное письмо МОиН РФ №03-296 от 12 мая 2011г. «Об организации внеурочной деятельности при введении федерального государственного образовательного стандарта общего образования»;
- Письмо МОиН РФ от 14 декабря 2015 года №09-3564 «О внеурочной деятельности и реализации дополнительных образовательных программ»;
- Письмо МОиН Самарской области от 17.02.2016 №МО-16-09-01/173-ТУ «О внеурочной деятельности».
- Авторской программы «Информационная безопасность или на расстоянии одного вируса» разработанной Наместниковой М.С.

Основными **целями** изучения курса «Информационная безопасность» являются:
1. обеспечение условий для профилактики негативных тенденций в информационной культуре учащихся, повышения защищенности детей от информационных рисков и угроз;
2. формирование навыков своевременного распознавания онлайн-рисков (технического, контентного, коммуникационного, потребительского характера и риска интернет-зависимости).

Задачи программы:

1**.** 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)**;**
2. 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;

3. 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.;
4. 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;
5. сформировать навыки по профилактике и коррекции зависимого поведения школьников, связанного с компьютерными технологиями и Интернетом.

Формы занятий: игры, лекции, беседы

Формы контроля: проекты, тестирования.

Данный курс предполагает изучение Модуля 1 (для обучающихся) авторской программы «Информационная безопасность или на расстоянии одного вируса», разработанной Наместниковой М.С., в течение одного года для обучающихся 8-х классов.
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 курса внеурочной деятельности
«Информационная безопасность» отводится по 1 часу в неделю в 8 классах.

Личностные, метапредметные и предметные результаты освоения учебного курса

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 использованиеминдивидуальных 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 безопасностижизнедеятельности;
- 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 решениязадачи/достижения цели;

- составлять план решения проблемы (выполнения проекта, проведения исследования);
- описывать свой опыт, оформляя его для передачи другим людям в виде технологии решенияпрактических задач определенного класса;
- оценивать свою деятельность, аргументируя причины достижения или отсутствия планируемогорезультата;
- находить достаточные средства для выполнения учебных действий в изменяющейся ситуации и/или приотсутствии 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 причиныи следствия явлений;
- строить рассуждение от общих закономерностей к частным явлениям и от частных явлений к общимзакономерностям;
- излагать полученную информацию, интерпретируя ее в контексте решаемой задачи;
- самостоятельно указывать на информацию, нуждающуюся в проверке, предлагать и применять способпроверки 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 своегомнения (если оно таково) и корректировать его;
- договариваться о правилах и вопросах для обсуждения в соответствии с поставленной перед группойзадачей;
- делать оценочный вывод о достижении цели коммуникации непосредственно после завершениякоммуникативного контакта и обосновывать его.
- целенаправленно искать и использовать информационные ресурсы, необходимые для решения учебныхи практических задач с помощью средств ИКТ;
- выбирать, строить и использовать адекватную информационную модель для передачи своих мыслейсредствами 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.

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 исообществах;
- сформированность понимания ценности безопасного образа жизни; интериоризация правил индивидуального и коллективного безопасного поведения в информационно-телекоммуникационнойсреде.

Содержание программы

Основное содержание программы представлено разделами «Безопасность общения», «Безопасность устройств», «Безопасность информации».

Каждый раздел курса внеурочной деятельности завершается выполнением проектной работы по одной из тем, предложенных на выбор учащихся и/или проверочного теста.

Раздел 1. «Безопасность общения»

Тема 1. Общение в социальных сетях и мессенджерах.

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

Пользовательский контент.

Тема 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.

Тема 3. Пароли для аккаунтов социальных сетей.

Сложные пароли. Онлайн генераторы паролей. Правила хранения паролей. Использование функции браузера позапоминанию паролей.

Тема 4. Безопасный вход в аккаунты.

Виды аутентификации. Настройки безопасности аккаунта. Работа на чужом компьютере с точки зрениябезопасности личного аккаунта.

Тема 5. Настройки конфиденциальности в социальных сетях.

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

Тема 6. Публикация информации в социальных сетях.

Персональные данные. Публикация личной информации.

Тема 7. Кибербуллинг.

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

Тема 8. Публичные аккаунты.

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

Тема 9. Фишинг.

Обзор фишинговых сайтов. Как защититься от фишеров в социальных сетях и мессенджерах.

Выполнение и защита индивидуальных и групповых проектов.

Раздел 2. «Безопасность устройств»

Тема 1. Что такое вредоносный код.

Виды вредоносных кодов. Возможности и деструктивные функции вредоносных кодов.

Тема 2. 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 об-наружении вредоносных кодов на устройствах.

Тема 3. Методы защиты от вредоносных программ.

Способы защиты устройств от вредоносного кода. Антивирусные программы и их характеристики. Правила защитыот вредоносных кодов.

Тема 4. Распространение вредоносного кода для мобильных устройств.

Расширение вредоносных кодов для мобильных устройств. Правила без-опасности при установке приложений намобильные устройства.

Выполнение и защита индивидуальных и групповых проектов.

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 социальныхролей. 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.

Безопасность личной информации. Создание резервных копий на различных устройствах.

Тема 6. Основы государственной политики в области формирования культуры информационнойбезопасности.

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

№	Наименование раздела	Количество часов
1	Безопасность общения	13
2	Безопасность устройств	8
3	Безопасность информации	13
	итого	34