государственное бюджетное общеобразовательное учреждение Самарской области основная общеобразовательная школа с. Купино муниципального района Безенчукский Самарской области

Проверено зам. директор по УВР Ефремова А.И. Протокол № 7 от «30» августа 2023г.	УТВЕРЖДАЮ директор ГБОУ ООШ с. Купино Пр. №140-од от 30.08.2023г. _____ Климова Л.В.

РАБОЧАЯ ПРОГРАММА

Предмет (курс) «Информационная безопасность» Класс 9

Количество часов по учебному плану: 34ч (1 ч в неделю)

Подписан: Климова Людмила Васильевна
DN: C=RU, OU=Директор, O=ГБОУ ООШ с.Купино, CN=Климова Людмила Васильевна, E=kupin_sch_bzn@samara.edu.ru
Основание: Я являюсь автором этого документа
Дата: 2023.11.08 16:13:14+04'00'

Рассмотрена на заседании МО учителей предметников

Протокол №1 от «30» августа 2023г.

Председатель МО Смирнова О.В.

Пояснительная записка

Программа разработана на основе:

- федерального государственного образовательного стандарта основного общего образования по предметным образовательным областям

«Математика и информатика», «Физическая культура и основы безопасности жизнедеятельности»;

- Примерной рабочей программы учебного курса «Цифровая гигиена» основного общего образования, рекомендованного Координационным

советом учебно-методических объединений в системе общего образования Самарской области (протокол № 27 от 21.08.2019);

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:

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 информационнотелекоммуникационной 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.

Общая характеристика учебного курса

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.

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 7-9 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 7, 8, 9 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 измененийситуации 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 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 завершениякоммуникативного 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 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,
созданиепрезентаций 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, обоснованноосуществлять 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 познава-тельных 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.

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. Для проведения занятий могут быть использованы презентации, проекты, памятки, онлайн занятия, подготовленные входе 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 всоциальных 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 позапоминанию паролей.

Тема 4. Безопасный вход в аккаунты. 1 час

Виды аутентификации. Настройки безопасности аккаунта. Работа на чужом компьютере с точки зрениябезопасности 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 жертвойкибербуллинга. 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 проектов3. 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 об-наружении 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 намобильные устройства.

Выполнение и защита индивидуальных и групповых проектов. 3 часа

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 социальныхролей. 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

Повторение.

Волонтерская практика. 3 часа

Тематическое планирование
курса внеурочной деятельности «Информационная безопасность» в 9 классе на 2021/2022 уч. год

№ п/ п	Т е м а	Кол во часов	Примерные сроки проведения	Основное содержание	Форма проведения
Тема 1. «Безопасность общения»					
1	Общение в социальных сетях и мессенджерах	1	Социальная сеть. История социальных сетей. Мессенджеры. Назначение социальных сетей и мессенджеров. Пользовательскийконтент.	Выполняет базовые операции при использовании мессенджеров и социальных сетей. Создает свой образ в сети Интернет. Изучает историю и социальную значимость личных аккаунтов в сети Интернет.	Беседа, практическая работа
2	С кем безопасно общаться в интернете	1	Персональные данные как основной капитал личного пространства в цифровом мире.	Руководствуется в общении социальными ценностями и	Беседа, практическая работа

			Правила добавления друзей в социальных сетях. Профиль пользователя. Анонимные социальные сети.	установками коллектива и общества в целом. Изучает правила сетевого общения.	
3	Пароли для аккаунтов социальных сетей	1	Сложные пароли. Онлайн генераторы паролей. Правила хранения паролей. Использование функции браузера по запоминанию паролей.	Изучает основные понятия регистрационной информации и шифрования. Умеет их применить.	Беседа, практическая работа
4	Безопасный вход в аккаунты	1	Виды аутентификации. Настройки безопасности аккаунта. Работа на чужом компьютере с точки зрения безопасности личного аккаунта.	Объясняет причины использования безопасного входа при работе на чужом устройстве. Демонстрирует устойчивый навык безопасного входа.	Беседа, практическая работа

5	Настройки конфиденциальности в социальных сетях	1	Настройки приватности и конфиденциальности в разных социальных сетях. Приватность и конфиденциальность в мессенджерах.	Раскрывает причины установки закрытого профиля. Меняет основные настройки приватности в личном профиле.	Беседа, практическая работа

6	Публикация информации в социальных сетях	1	Персональные данные. Публикация личной информации.	Осуществляет поиск и использует информацию, необходимую для выполнения поставленных задач.	Беседа, практическая работа
7	Кибербуллинг	1	Определение кибербуллинга. Возможные причины кибербуллинга и как его избежать? Как не стать жертвой кибербуллинга. Как помочь жертве кибербуллинга.	Реагирует на опасные ситуации, распознает провокации и попытки манипуляции со стороны виртуальных собеседников.	Беседа, практическая работа
8	Публичные аккаунты	1	Настройки приватности публичных страниц. Правила ведения публичных страниц. Овершеринг.	Решает экспериментальные задачи. Самостоятельно создает источники информации разного типа и для разных аудиторий, соблюдая правила информационной безопасности.	Беседа, практическая работа
9	Фишинг	2	Фишинг как мошеннический прием. Популярные варианты распространения	Анализ проблемных ситуаций. Разработка кейсов с примерами из личной	Беседа, практическая работа

			фишинга. Отличие настоящих и фишинговых сайтов. Как защититься от фишеров в социальных сетях и мессенджерах.	жизни/жизни знакомых. Разработка и распространение чек листа (памятки) по противодействию фишингу.	
10	Выполнение и защита индивидуальных и групповых проектов	3	Самостоятельная работа.		Беседа, практическая работа
Тема 2. «Безопасность устройств»					
1	Что такое вредоносный код?	1	Виды вредоносных кодов. Возможности и деструктивные функции вредоносных кодов.	Соблюдает технику безопасности при эксплуатации компьютерных систем. Использует инструментальные программные средства и сервисы адекватно задаче.	Беседа, практическая работа
2	Распространение вредоносного кода	1	Способы доставки вредоносных кодов. Исполняемые файлы и расширения вредоносных кодов.	Выявляет и анализирует (при помощи чек-листа) возможные угрозы информационной безопасности объектов.	Беседа, практическая работа

			Вредоносная рассылка. Вредоносные скрипты. Способы выявления наличия вредоносных кодов на устройствах. Действия при обнаружении вредоносных кодов на устройствах.		
3	Методы защиты от вредоносных программ	2	Способы защиты устройств от вредоносного кода. Антивирусные программы и их характеристики. Правила защиты от вредоносных кодов.	Изучает виды антивирусных программ и правила их установки.	Беседа, практическая работа
4	Распространение вредоносного кода для мобильных устройств	1	Расширение вредоносных кодов для мобильных устройств. Правила безопасности при установке приложений на мобильные	Разрабатывает презентацию, инструкцию по обнаружению, алгоритм установки приложений на мобильные устройства для учащихся более	Беседа, практическая работа

			устройства.	младшего возраста.	
5	Выполнение и защита индивидуальных и групповых проектов	3	Умеет работать индивидуально и в группе. Принимает позицию собеседника, понимая позицию другого, различает в его речи: мнение (точку зрения), доказательство (аргументы), факты; гипотезы, аксиомы, теории.		Беседа, практическая работа
Тема 3 «Безопасность информации»					
1	Социальная инженерия: распознать и избежать	1	Приемы социальной инженерии. Правила безопасности при виртуальных контактах.	Находит нужную информацию в базах данных, составляя запросы на поиск. Систематизирует получаемую информацию в процессе поиска.	Беседа, практическая работа

2	Ложная информация в Интернете	1	Цифровое пространство как площадка самопрезентации, экспериментирования и освоения различных социальных ролей. Фейковые новости. Поддельные страницы.	Определяет возможные источники необходимых сведений, осуществляет поиск информации. Отбирает и сравнивает материал по нескольким источникам. Анализирует и оценивает достоверность информации.	Беседа, практическая работа
3	Безопасность при использовании платежных карт в Интернете	1	Транзакции и связанные с ними риски. Правила совершения онлайн покупок. Безопасность банковских сервисов.	Приводит примеры рисков, связанных с совершением онлайн покупок (умеет определить источник риска). Разрабатывает возможные варианты	Беседа, практическая работа
решения ситуаций, связанных с рисками использования платежных карт в Интернете.					Беседа, практическая работа
4	Беспроводная	1	Уязвимость Wi-Fi-	Используя	Беседа,

	технология связи		соединений. Публичные и непубличные сети. Правила работы в публичных сетях.	различную информацию, определяет понятия. Изучает особенности и стиль ведения личных и публичных аккаунтов.	практическая работа
5	Резервное копирование данных	1	Безопасность личной информации. Создание резервных копий на различных устройствах.	Создает резервные копии.	Беседа, практическая работа
6	Основы государственной политики в области формирования культуры информационной безопасности	2	Доктрина национальной информационной безопасности. Обеспечение свободы и равенства доступа к информации и знаниям. Основные направления государственной политики в области формирования культуры информационной безопасности.	Умеет привести выдержки из законодательства РФ: - обеспечивающего конституционное право на поиск, получение и распространение информации; - отражающего правовые аспекты защиты киберпространства.	Беседа, практическая работа

7	Выполнение и защита индивидуальных и групповых проектов	3	Самостоятельная и групповая работа по созданию продукта проекта		Беседа, практическая работа
8	Повторение, волонтерская практика, резерв	3			Беседа, практическая работа
Итого:	**34 часа**				

Требования к содержанию итоговых проектно-исследовательских работ

Критерии содержания текста проектно-исследовательской работы

1. Во введении сформулирована актуальность (личностная и социальная значимость) выбранной проблемы. Тема может быть переформулирована,
но при этом четко определена, в необходимости исследования есть аргументы.
2. Правильно составлен научный аппарат работы: точность формулировки проблемы, четкость и конкретность впостановке цели и задач,
определении объекта и предмета исследования, выдвижении гипотезы. Гипотеза сформули-рована корректно и соответствуют теме работы.
3. Есть планирование проектно-исследовательской деятельности, корректировка ее в зависимости от результатов, получаемых на разных
этапах развития проекта. Дана характеристика каждого этапа реализации проекта,
сформулированы задачи, которые решаются на каждом этапе, в
случае коллективного проекта - распределены и выполнены задачи каждым участником, анализ ресурсного обеспечения проекта проведен
корректно.
4. Используется и осмысляется междисциплинарный подход к исследованию и проектированию и на базовом уровне школьной программы,
и на уровне освоения дополнительных библиографических источников.
5. Определён объём собственных данных и сопоставлено собственное проектное решение с аналоговыми по проблеме. Дан анализ
источников и аналогов с точки зрения значимости для собственной проектно- исследовательской работы, выявлена его новизна, библиография и
интернет ресурсы грамотно оформлены.
6. Соблюдены нормы научного стиля изложения и оформления работы. Текст работы должен

демонстрировать уровень владения научным
стилем изложения.
7. Есть оценка результативности проекта, соотнесение с поставленными задачами. Проведена оценка социокультурных и образовательных
последствий проекта на индивидуальном и общественном уровнях.

Критерии презентации проектно-исследовательской работы (устного выступления).

1. Демонстрация коммуникативных навыков при защите работы. Владение риторическими умениями, раскрытие автором содержание
работы, достаточная осведомленность в терминологической системе проблемы, отсутствие стилистических и речевых ошибок, соблюдение
регламента.
2. Умение чётко отвечать на вопросы после презентации работы.
3. Умение создать качественную презентацию. Демонстрация умения использовать IT-технологии и создавать слайдпрезентацию на
соответствующем его возрасту уровне.
4. Умение оформлять качественный презентационный буклет на соответствующем его возрасту уровне.
5. Творческий подход к созданию продукта, оригинальность, наглядность, иллюстративность. Предоставлен качественный творческий
продукт (макет, программный продукт, стенд, статья, наглядное пособие, литературное произведение, видеоролик, мультфильм и т.д.).
6. Умение установить отношения коллаборации с участниками проекта, наметить пути создания сетевого продукта. Способность намечать
пути сотрудничества на уровне взаимодействия с членами кружка или секции, проявление в ходе презентации коммуникабельности,
благодарности и уважения по отношению к руководителю, консультантам, умение
четко обозначить пути создания сетевого продукта.
7. Ярко выраженный интерес к научному поиску, самостоятельность в выборе проблемы, пути ее исследования и проектного решения.