государственное бюджетное общеобразовательное учреждение Самарской области
средняя общеобразовательная школа пос.Октябрьский городского округа Похвистнево
Самарской области

Рассмотрена и принята **Утверждена**

На педагогическом совете школы приказом директора школы
Протокол № 7 от 31.05.2023г. № 38/5 – од от «01» июня 2023 г.
Директор _____ / Пахомова Т.А. /
(подпись) (ФИО)

РАБОЧАЯ ПРОГРАММА

по внеурочной деятельности

«Информационная безопасность»

на 2023-2024 учебный год

(*на уровень основного общего образования*)

Составитель:
Рыблова Н.В.,
учитель изобразительного искусства

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»;
- Учебного плана внеурочной деятельности ГБОУ СОШ пос.Октябрьский г.о.Похвистнево на 2023-2024 учебный год;
- Примерной рабочей программы учебного курса «Цифровая гигиена» основного общего образования, рекомендованного Координационным советом учебно-методических объединений в системе общего образования Самарской области.

Основными **целями** изучения курса «Информационная безопасность» являются:

- обеспечение условий для профилактики негативных тенденций в информационной культуре учащихся, повышения защищенностидетей 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 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.

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 уровня основного общего образования.

На изучение курса внеурочной деятельности «Информационная безопасность» отводится 34 учебных часа, по 1 часу в неделю, на уровень основного общего образования.

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 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 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 определенногокласса;
- 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 достоверностиинформации;

•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) икорректировать 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 иобосновывать 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 правилаинформационной 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.
-

Тематическое планирование

Раздел	Наименование раздела	Количество часов
Тема 1.	«Безопасность общения»	13 часов
Тема 2.	«Безопасность устройств»	8 часов
Тема 3.	«Безопасность информации»	13 часов

Календарно-тематическое планирование
курса внеурочной деятельности «Информационная безопасность» в 7 классе на 2023/2024 уч. год

№ п/п	**Тема**	Кол- во часов	срок проведения	Основное содержание	Характеристика основных видов учебной деятельности обучающихся
			Раздел 1. «Безопасность общения»		
1	Общение в социальных сетях имессенджерах	1		Социальная сеть. История социальныхсетей. Мессенджеры. Назначение социальных сетей и мессенджеров. Пользовательский контент.	Выполняет базовые операции при использовании мессенджеров и социальных сетей. Создает свой образ всети Интернет. Изучает историю и социальную значимость личных аккаунтов в сети Интернет.
2	С кем безопасно общаться в интернете	1		Персональные данные как основной капитал личного пространства в цифровоммире. Правила добавления друзей в социальных сетях.Профиль пользователя. Анонимные социальные сети.	Руководствуется в общении социальными ценностями и установками коллектива и общества вцелом. Изучает правила сетевого общения.
3	Пароли дляаккаунтов социальныхсетей	1		Сложные пароли. Онлайн генераторыпаролей. Правила хранения паролей. Использование функции браузера по запоминанию паролей.	Изучает основные понятия регистрационной информации и шифрования. Умеет их применить.
4	Безопасный вход в аккаунты	1		Виды аутентификации. Настройкибезопасности аккаунта. Работа на чужомкомпьютере с точки зрения безопасности личного аккаунта.	Объясняет причины использования безопасного входа при работе на чужомустройстве. Демонстрирует устойчивый навык безопасного входа.
5	Настройки конфиденциальности в социальных сетях	1		Настройки приватности и конфиденциальности в разных социальных сетях. Приватность иконфиденциальность в мессенджерах.	Раскрывает причины установки закрытого профиля. Меняет основныенастройки приватности в личном профиле.
6	Публикация информации в социальных сетях	1		Персональные данные. Публикацияличной информации.	Осуществляет поиск и используетинформацию, необходимую для выполнения поставленных задач.
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.
8	Публичные аккаунты	2		Настройки приватности публичныхстраниц. Правила ведения публичных страниц. Овершеринг.	Решает экспериментальные задачи. Самостоятельно создает источники информации разного типа и для разных аудиторий, соблюдая правила информационной безопасности.
9	Фишинг	2		Фишинг как мошеннический прием.Популярные варианты распространения фишинга. Отличиенастоящих и фишинговых сайтов.Как защититься от фишеров в социальных сетях и мессенджерах.	Анализ проблемных ситуаций. Разработка кейсов с примерами изличной жизни/жизни знакомых. Разработка и распространение чек- листа (памятки) по противодействию фишингу.
10	Выполнение и защита индивидуальных и групповых проектов	2			Самостоятельная работа.
ИТОГО:		13ч			
			Раздел 2. «Безопасность устройств»		
1	Что такое вредоносный	1		Виды вредоносных кодов. Возможности и деструктивные	Соблюдает технику безопасности приэксплуатации

	код?			функции вредоносных кодов.	компьютерных систем.Использует инструментальные программные средства и сервисы адекватно задаче.
2	Распространение вредоносного кода	1		Способы доставки вредоносныхкодов. Исполняемые файлы и расширения вредоносных кодов.Вредоносная рассылка. Вредоносные скрипты. Способы выявления наличия вредоносных кодов на устройствах. Действия при обнаружении вредоносных кодов наустройствах.	Выявляет и анализирует (при помощичек-листа) возможные угрозы информационной безопасности объектов.
3	Методы защиты от вредоносных программ	2		Способы защиты устройств от вредоносного кода. Антивирусныепрограммы и их характеристики. Правила защиты от вредоносныхкодов.	Изучает виды антивирусных программи правила их установки.
4	Распространение вредоносного кода для мобильных устройств	1		Расширение вредоносных кодов длямобильных устройств. Правила безопасности при установке приложений на мобильныеустройства.	Разрабатывает презентацию, инструкцию по обнаружению, алгоритм установки 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.
ИТОГО:		8ч			
Раздел 3. «Безопасность информации»					
1	Социальная инженерия: распознать и избежать	1		Приемы социальной инженерии.Правила безопасности при виртуальных контактах.	Находит нужную информацию в базахданных, составляя запросы на поиск. Систематизирует получаемую информацию в процессе поиска.
2	Ложная информация в Интернете	1		Цифровое пространство как площадка самопрезентации, экспериментирования и освоенияразличных социальных ролей. Фейковые новости. Поддельные страницы.	Определяет возможные источники необходимых сведений, осуществляетпоиск информации. Отбирает и сравнивает материал по нескольким источникам. Анализируетиоценивает достоверность информации.
3	Безопасность при использовании платежныхкарт в Интернете	1		Транзакции и связанные с ними риски. Правила совершения онлайнпокупок. Безопасность банковских сервисов.	Приводит примеры рисков, связанных ссовершением онлайн покупок (умеет определить источник риска). Разрабатывает возможные варианты решения ситуаций, связанных с рисками использования платежных карт в Интернете.
4	Беспроводная технология связи	1		Уязвимость Wi-Fi-соединений. Публичные и непубличные сети. Правила работы в публичных сетях.	Используя различную информацию, определяет понятия. Изучает особенности и стиль ведения личных ипубличных аккаунтов.
5	Резервное копирование данных	1		Безопасность личной информации. Создание резервных копий наразличных устройствах.	Создает резервные копии.
6	Основы государственной политики в области формирования культуры информационной безопасности	2		Доктрина национальной информационной безопасности. Обеспечение свободы и равенствадоступа к информации и знаниям.Основные направления государственной политики в области формирования культуры информационной безопасности.	Умеет привести выдержки иззаконодательства РФ: - обеспечивающего конституционноеправо на поиск, получение и распространение информации; - отражающего правовые аспектызащиты киберпространства.
7	Написание	3			Самостоятельная работа по созданию реферата

	индивидуальных рефератов				
8	Повторение, волонтерская практика, резерв	3			
ИТОГО:		13ч			
ИТОГО:		**34 часа**			