МИНИСТЕРСТВО ПРОСВЕЩЕНИЯ РОССИЙСКОЙ ФЕДЕРАЦИИ

Министерство образования Самарской области

Северное управление министерства образования Самарской области

Государственное бюджетное общеобразовательное учреждение Самарской области средняя общеобразовательная школа "Образовательный центр" с. Денискино муниципального района Шенталинский Самарской области

РАССМОТРЕНО	**ПРОВЕРЕНО**	**УТВЕРЖДЕНО**
Руководитель МО	Учитель	И.о. директора
_____	_____	_____
Мингазов Р.А.	Щербакова Р.А.	Нуртдинов А.Р.
Протокол № 1 от "25" августа 20256г.	"25" августа 2026 г.	Приказ № 55-од от 25.08.2026 г.

РАБОЧАЯ ПРОГРАММА КУРСА

««ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ ИЛИ НА РАССТОЯНИИ ОДНОГО ВИРУСА»

для обучающихся 7 класса

Денискино, 2025

Пояснительная записка

Основными целями изучения курса внеурочной деятельности ««Информационная безопасность или на расстоянии одного вируса» 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.

Общая характеристика учебного курса

Курс ««Информационная безопасность или на расстоянии одного вируса» является важной составляющей работы с обучающимися по «Цифровой гигиене», 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 создаст условия для

сокращения цифрового разрыва между поколениями и позволит родителям выступать в качестве экспертов, передающих опыт.

Данный курс предполагает организацию работы в соответствии с содержанием 2-х модулей, предназначенных для обучающихся 7-9 классов и родителей обучающихся любого возраста соответственно.

Модуль 1.

Отбор тематики содержания курса осуществлен с учетом целей и задач ФГОС основного общего образования, возрастных особенностей и познавательных возможностей обучающихся 7-9 классов.

В преподавании курса ««Информационная безопасность или на расстоянии одного вируса» » могут использоваться разнообразные форматы обучения: традиционный (коллективная и групповая формы работы), тренинги (в классической форме или по кейс- методу), дистанционное обучение (электронные курсы, видеоролики, почтовые рассылки, микрообучение), смешанный формат.

Система заданий должна создавать 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 учащихся, 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.).

Место курса (Модуль 1) в учебном плане

Программа курса (Модуль 1) рассчитана на 34 учебных часа, из них 22 часа – занятий, 9 часов – подготовка и защита учебных проектов, 3 часа – повторение. На изучение модуля 1 курса «Информационная безопасность или на расстоянии одного вируса» отводится по 1 часу в неделю в 7 классах, Занятия по программе могут быть реализованы в различных вариантах:

1) в течение одного учебного года в 7 классах. В этом случае программа рассчитана на 34 учебные недели;
2) по одному разделу последовательно в 7 классах;
3) произвольно распределены учителем в зависимости от интереса и готовности школьников.

Характеристика личностных, метапредметных и предметных результатов освоения 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 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.

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 ценности безопасного образа жизни; интериоризация правил индивидуального и коллективного безопасного поведения в информационно-телекоммуникационной среде.

Содержание программы курса (Модуль 1).

Содержание программы курса (Модуль 1) соответствует темам основной образовательной программы основного общего образования по учебным предметам «Информатика» и «ОБЗР», 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 (Модуля 1) 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.

Содержание курса (Модуль 1).
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]. 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.

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.

Повторение. Волонтерская практика. 3 часа.

Тематическое планирование курса .

№ п/п	Тема	Количество часов	Основное содержание
Тема 1. «Безопасность общения»			
1	Общение в социальных сетях и мессенджерах	1	Социальная сеть. История социальных Мессенджеры. Назначение соци мессенджеров. Пользовательский контент.
2	С кем безопасно общаться в интернете	1	Персональные данные как осно пространства в цифровом мире. Пра социальных сетях. Профиль пользователя. Анонимные соци
3	Пароли для аккаунтов социальных сетей	1	Сложные пароли. Онлайн генерат хранения паролей. Использование функции бра паролей.

4	Безопасный вход в аккаунты	1	Виды аутентификации. Наст аккаунта. Работа на чужом ком безопасности личного аккаунта.
5	Настройки конфиденциальности в социальных сетях	1	Настройки приватности и конфи социальных сетях. Приватность и конфиденциальность в месс
6	Публикация информации в социальных сетях	1	Персональные данные. Публикация личной инфо
7	Кибербуллинг	1	Определение кибербуллинга. Возмож кибербуллинга и как его избежать? Ка кибербуллинга. Как помочь жертве ки
8	Публичные аккаунты	1	Настройки приватности пуб ведения публичных страниц. Овершер

9	Фишинг	2	Фишинг как мошеннический при распространения фишинга. Отли фишинговых сайтов. Как защититься с сетях и мессенджерах.
	Выполнение и защита индивидуальных и групповых проектов	3	
Тема 2. «Безопасность устройств»			
1	Что такое вредоносный код	1	Виды вредоносных кодов. Возможнос вредоносных кодов.
2	Распространение вредоносного кода	1	Способы доставки вредоносных код расширения вредоносных кодов. Вред Вредоносные скрипты. Способы выявления наличия вредоносных

			кодов на устройствах. Действия при обнаружении вредоносных кодов
3	Методы защиты от вредоносных программ	2	Способы защиты устройств от вредоно программы и их характеристики. Прав от вредоносных кодов.
4	Распространение вредоносного кода для мобильных устройств	1	Расширение вредоносных кодов д Правила безопасности при установке устройства.
	Выполнение и защита индивидуальных и групповых проектов	3	
Тема 3 «Безопасность информации»			
1	Социальная инженерия: распознать и избежать	1	Приемы социальной инженерии. Прав при виртуальных контакт

2	Ложная информация в Интернете	1	Цифровое пространство как п экспериментирования и освоения ра Фейковые новости. Поддельные стран
3	Безопасность при использовании платежных карт в Интернете	1	Транзакции и связанные с ними риски покупок. Безопасность банковских сер
4	Беспроводная технология связи	1	Уязвимость Wi-Fi-соединений. Публ Правила работы в публичных сетях.
5	Резервное копирование данных	1	Безопасность личной ин

			резервных копий на различных уст
6	Основы государственной политики в области формирования культуры информационной безопасности	2	Доктрина национальной инф Обеспечение свободы и равенства знаниям. Основные на политики в области фор информационной безопасности.
	Выполнение и защита индивидуальных и групповых проектов	3	
	Повторение, волонтерская практика, резерв	3	
	Итого	34	

Модуль 2.

При работе с родителями важнейшей задачей является преодоление «цифрового разрыва» и обучение родителей правильной оценке своих возможностей в помощи детям в Интернете – возможностей, которые достаточно велики.

Разработчики курса предполагают, что родители с бóльшей готовностью включатся в программу развития цифровой гигиены, предлагающую им общение, совместный поиск и развивающие игры и т.п.

Вместе с тем, формами проведения мероприятий для родителей также могут являться: лектории, выступления на родительских собраниях, микрообучение на основе технологий онлайн обучения, геймификация, создание чек-листов, совместное обучение, совместные родительско-детские проекты и пр.

Практические материалы для реализации данного модуля представлены в приложении 2 к данной рабочей программе. Разработчики курса ««Информационная безопасность или на расстоянии одного вируса» » предлагают использовать вышеуказанное приложение в качестве конструктора при подготовке к мероприятиям.

Тематическое планирование учебного курса .

Тема 1. История возникновения Интернета. Понятия Интернет-угроз. Изменения границ допустимого в контексте цифрового образа жизни

Тема 2. Изменения нормативных моделей развития и здоровья детей и подростков.

Тема 3. Цифровая гигиена: зачем это нужно? Понятие периметра безопасности. Баланс ценностей развития и ценностей безопасности.

Тема 4. Угрозы информационной безопасности: атаки, связанные с компьютерной инженерией. Способы выявления наличия вредоносных кодов на устройствах. Действия при обнаружении вредоносных кодов на устройствах.

Тема 5. Угрозы информационной безопасности: атаки, связанные с социальной инженерией. Груминг, кибербуллинг. Чему мы должны научить ребёнка для профилактики насилия в Сети?

Тема 6. Угрозы информационной безопасности: атаки, связанные с социальной инженерией. Фишинг. Обращение с деньгами в сети Интернет. Детская пластиковая карта: быть или не быть?

Тема 7. Обеспечение эмоционально-психологического периметра безопасности в соответствии с возрастными особенностями ребенка.

Тема 8. Контентные риски. Настройка и безопасное использование смартфона или планшета. Семейный доступ.

Тема 9. Пособия и обучающие программы по формированию навыков цифровой гигиены.

Список источников:

1. Бабаш, А.В. «Информационная безопасность или на расстоянии одного вируса» : Лабораторный практикум / 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 закон, 2014. – 182 с.
3. Громов, Ю.Ю. «Информационная безопасность или на расстоянии одного вируса» 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 или на расстоянии одного вируса» детей. Российский и зарубежный опыт: Монография / Л.Л. Ефимова, С.А. Кочерга. – М.: ЮНИТИ- ДАНА, 2016. – 239 с.
6. Запечников, С.В. «Информационная безопасность или на расстоянии одного вируса» 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 безопасность или на расстоянии одного вируса» общества / А.В. Кузнецова, С.И. Самыгин, М.В. Радионов. – М.: Русайнс, 2017. – 64 с.
9. Основы кибербезопасности. // https://www.xn--d1abkefqip0a2f.xn--p1ai/index.php/glava-1-osnovy-kiberbezopasnosti-tseli-i-zadachi-kursa
10. Стрельцов А.А. Правовое обеспечение информационной безопасности России: теоретические и методологические основы. – Минск, 2005. – 304 с.
11. Сусоров И.А. Перспективные технологии обеспечения кибербезопасности // Студенческий: электрон. научн. журн. 2019. № 22(66)
12. Цифровая компетентность подростков и родителей. Результаты всероссийского исследования / Г.У. Солдатова, Т.А. Нестик, Е.И. Рассказова, Е.Ю. Зотова. – М.: Фонд Развития Интернет, 2013. – 144 с.