МИНИСТЕРСТВО ПРОСВЕЩЕНИЯ РОССИЙСКОЙ ФЕДЕРАЦИИ
министерство образования Самарской области Северное управление
Государственное бюджетное общеобразовательное учреждение Самарской области средняя общеобразовательная школа № 1 п.г.т.Суходол муниципального района Сергиевский Самарской области

РАССМОТРЕНО	СОГЛАСОВАНО	УТВЕРЖДЕНО
Руководитель МО	Заместитель директора	Директор школы
Котельникова О.В.	по УВР Котельникова О.В.	Соломонова Т.В.
«26» августа 2025 г.	«28» августа 2025 г.	№163-од от «29» августа 2025 г.

ЭП

C=RU, OU=директор, O=ГБОУ СОШ № 1 п.г.т. Суходол, CN=Соломонова Татьяна Владимировна, E=su.suhodol_sch1@63edu.ru
00a2864f5788709768
2025.08.30 16:03:20+04'00'

РАБОЧАЯ ПРОГРАММА

курса внеурочной деятельности

«Информационная безопасность, или на расстоянии одного вируса»

для обучающихся 7 классов

Разработчик:
Моисеева О.Н.,
учитель

СУХОДОЛ, 2025

Пояснительная записка

Рабочая программа кружка по внеурочной деятельности «Информационная безопасность или на расстоянии одного вируса» для учащихся 7-9 классов подготовлена на основе:

- Федерального государственного образовательного стандарта основного общего образования (Приказ Минпросвещения России от 31.05.2021 г. № 287);
- «Положение об организации внеурочной деятельности», утвержденное приказом директора № 69/5 от 18.04.2019 г.;
- Письмо МОиН РФ №03-296 от 12.05.2011 г «Об организации внеурочной деятельности при введении федерального государственного образовательного стандарта общего образования»;
- Основная образовательная программа основного общего образования ГБОУ СОШ № 1 п.г.т. Суходол.

Образовательный процесс осуществляется с использованием учебников, учебных пособий, входящих в действующий федеральный перечень. Перечень учебников ежегодно утверждается приказом директора школы.

Программа кружка «Информационная безопасность или на расстоянии одного вируса» разработана с учётом современных мировых требований внеурочной деятельности в 7-9 классах. В рабочей программе учтены идеи и положения Концепции развития духовно-нравственного воспитания российских школьников, требований Федерального государственного образовательного стандарта начального общего образования, «Планируемых результатов среднего общего образования».

Курс является важной составляющей частью работы с учащимися, активно использующими различные сетевые формы общения (социальные сети, игры, пр.), задумывающимися о своей личной безопасности, безопасности своей семьи и своих друзей, а также проявляющими интерес к изучению истории и технологических основ информационной безопасности.

Направление программы курса внеурочной деятельности – общеинтеллектульное. Программа курса ориентирована на выполнение требований Федерального государственного образовательного стандарта основного общего образования к организации и содержанию внеурочной деятельности школьников. Ее реализация даёт возможность раскрытия индивидуальных способностей школьников, развития интереса к различным видам индивидуальной и групповой деятельности, закрепления умения самостоятельно организовать свою учебную, в том числе проектную деятельность.

Формирование активной позиции школьников в получении знаний и умений выявлять информационную угрозу, определять степень ее опасности, предвидеть последствия информационной угрозы и противостоять им. Обеспечение условий для профилактики негативных тенденций в информационной культуре учащихся, повышения защищенности детей от информационных рисков и угроз

Данная программа представляет собой определенную систему содержания, форм, методов и приемов педагогических воздействий, опирается на принципы индивидуализации, взаимодействия личности и коллектива, развивающего воспитания и единства образовательной и воспитательной среды.

Программа кружка «Информационная безопасность или на расстоянии одного вируса» предназначена для учащихся 7-9 классов средней общеобразовательной школы.
Количество часов: в неделю – 1ч; в год – 34 ч.

Цели и особенности изучения кружка
«Информационная безопасность или на расстоянии одного вируса»
7 – 9 классы.

На основе национального воспитательного идеала формулируется основная педагогическая цель – воспитание нравственного, ответственного, инициативного и компетентного гражданина России.
Воспитание гражданина страны - одно из главных условий национального возрождения. Функционально грамотный гражданин - это человек, любящий Родину, умеющий реагировать на изменения в обществе, защищать свое человеческое право. Понятие ГРАЖДАНСТВЕННОСТЬ предполагает освоение и реализацию ребенком своих прав и обязанностей по отношению к себе самому, своей семье, коллективу, к родному краю, Отечеству, планете Земля. Важно воспитать деятельного гражданина своей Родины, а не стороннего наблюдателя. Формируя гражданина, мы, прежде всего, должны видеть в нем человека. Поэтому гражданин с педагогической точки зрения - это самобытная индивидуальность, личность, обладающая единством духовно-нравственного и правового долга.

Цель программы:

- формирование активной позиции школьников в получении знаний и умений выявлять информационную угрозу, определять степень ее опасности, предвидеть последствия информационной угрозы и противостоять им;
- обеспечение условий для профилактики негативных тенденций в информационной культуре учащихся, повышения защищенности детей от информационных рисков и угроз.

Для достижения указанной цели решаются следующие задачи:

- дать представление о современном информационном обществе, информационной безопасности личности и государства;
- сформировать навыки ответственного и безопасного поведения современной информационно-телекоммуникационной среде;
- сформировать навыки по профилактике и коррекции зависимого поведения школьников, связанного с компьютерными технологиями и Интернетом;

• сформировать общекультурные навыки работы с информацией (умений грамотно пользоваться источниками информации, правильно организовать информационный процесс);
• дать представление о видах и способах распространения вредоносных кодов, способов защиты личных устройств;
• познакомить со способами защиты от противоправных посягательств в сети Интернет, защиты личных данных.

В ходе изучения учебного курса обучающиеся усовершенствуют опыт проектной деятельности и навыки работы с информацией, в том числе в текстовом, табличном виде, виде диаграмм, теоретические и практические занятия для самостоятельного принятия решения и осуществления осознанного выбора в учебной и познавательной деятельности при формировании современной культуры безопасности в сети интернет.

Освоение курса «Информационная безопасность или на расстоянии одного вируса» должно обеспечивать достижение на уровне основного общего образования следующих личностных, метапредметных и предметных образовательных результатов:

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 ценности безопасного образа жизни; интериоризация правил индивидуального и коллективного безопасного поведения в информационнотелекоммуникационной среде.

• развитие морального сознания и компетентности в решении моральных проблем на основе личностного выбора, формирование нравственных чувств и нравственного поведения, осознанного и ответственного отношения к собственным поступкам;

• формирование коммуникативной компетентности в общении и сотрудничестве со сверстниками, детьми старшего и младшего возраста, взрослыми в процессе образовательной, общественно полезной, учебно-исследовательской, творческой и других видов деятельности;

Метапредметные результаты:

- умение самостоятельно определять цели своего обучения, ставить и формулировать для себя новые задачи в познавательной деятельности, развивать мотивы и интересы своей познавательной деятельности;

- умение самостоятельно планировать пути достижения целей, в том числе альтернативные, осознанно выбирать наиболее эффективные способы решения учебных и познавательных задач;

- умение соотносить свои действия с планируемыми результатами, осуществлять контроль своей деятельности в процессе достижения результата, определять способы действий в рамках предложенных условий и требований, корректировать свои действия в соответствии с изменяющейся ситуацией;

- владение основами самоконтроля, самооценки, принятия решений и осуществления осознанного выбора в познавательной деятельности;

- 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;

- формулировать учебные задачи как шаги достижения поставленной цели деятельности;

- обосновывать целевые ориентиры и приоритеты ссылками на ценности, указывая и обосновывая логическую последовательность шагов;

- определять необходимые действие(я) в соответствии с учебной и познавательной задачей и составлять алгоритм их выполнения;

- обосновывать и осуществлять выбор наиболее эффективных способов решения учебных и познавательных задач;

- определять/находить, в том числе из предложенных вариантов, условия для выполнения учебной и познавательной задачи;

- выстраивать жизненные планы на краткосрочное будущее (заявлять целевые ориентиры, ставить адекватные им задачи и предлагать действия, указывая и обосновывая логическую последовательность шагов);

- выбирать из предложенных вариантов и самостоятельно искать средства/ресурсы для решения задачи/достижения цели;

- составлять план решения проблемы (выполнения проекта, проведения исследования);

- определять потенциальные затруднения при решении учебной и познавательной задачи и находить средства для их устранения;

• описывать свой опыт, оформляя его для передачи другим людям в виде технологии решения практических задач определенного класса;

• определять совместно с педагогом и сверстниками критерии планируемых результатов и критерии оценки своей учебной деятельности;

• систематизировать (в том числе выбирать приоритетные) критерии планируемых результатов и оценки своей деятельности;

• умение организовывать учебное сотрудничество и совместную деятельность с учителем и сверстниками; работать индивидуально и в группе: находить общее решение и разрешать конфликты на основе согласования позиций и учета интересов; формулировать, аргументировать и отстаивать свое мнение;

Предметные результаты:

Научатся:

• 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;

Получат возможность

Овладеть:

• приемами безопасной организации своего личного пространства данных с использованием индивидуальных накопителей данных, интернет-сервисов и т.п;
• основами самоконтроля, соблюдения норм информационной этики и права;
• навыками самостоятельного принятия решения и осуществления осознанного выбора в учебной и познавательной деятельности при формировании современной культуры безопасности в сети интернет;

Содержание кружка
«Информационная безопасность или на расстоянии одного вируса»
7-9 классы.

7 класс

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 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 по запоминанию паролей.

Тема 4. Безопасный вход в аккаунты. Виды аутентификации. Настройки безопасности аккаунта. Работа на чужом компьютере с точки зрения безопасности личного аккаунта.

Тема 5. Настройки конфиденциальности в социальных сетях Настройки приватности и конфиденциальности в разных социальных сетях. Приватность и конфидициальность в месседжерах.

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 жертвой кибербуллинга. Как помочь жертве кибербуллинга.

Тема 8. Публичные аккаунты Настройки приватности публичных страниц. Правила ведения публичных страниц.

Тема 9. Фишинг Фишинг как мошеннический прием. Популярные варианты распространения фишинга. Отличие настоящих и фишинговых сайтов. Как защититься от фишеров в социальных сетях и мессенджерах.

Тема 10. Выполнение и защита индивидуальных и групповых проектов Проектная деятельность. Этапы выполнения проекта. Выбор темы проекта. Цели, задачи, SMART. Защита проекта.

8 КЛАСС

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 обнаружении вредоносных кодов на устройствах.

Тема 3. Методы защиты от вредоносных программ Способы защиты устройств от вредоносного кода. Антивирусные программы и их характеристики. Правила защиты от вредоносных кодов. *Тема 4*. Распространение вредоносного кода для мобильных устройств Расширение вредоносных кодов для мобильных устройств. Правила безопасности при установке приложений на мобильные устройства.

Тема 5. Выполнение и защита индивидуальных и групповых проектов Проектная деятельность. Этапы выполнения проекта. Выбор темы проекта. Цели, задачи, SMART. Защита проекта.

9 КЛАСС

БЕЗОПАСНОСТЬ ИНФОРМАЦИИ

Тема 1. Социальная инженерия: распознать и избежать. Приемы социальной инженерии. Правила безопасности в виртуальных контактах.

Тема 2. Ложная информация в Интернете 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 Уязвимости Wi-Fi-соединений. Публичные и непубличные сети. Правила работы в публичных сетях.

Тема 5. Резервное копирование данных Безопасность личной информации. Создание резервных копий на различных устройствах.

Тема 6. Выполнение и защита индивидуальных и групповых проектов Проектная деятельность. Этапы выполнения проекта. Выбор темы проекта. Цели, задачи, SMART. Защита проекта

ТЕМАТИЧЕСКОЕ ПЛАНИРОВАНИЕ

7 КЛАСС

Тематический блок/раздел	**Основное содержание**	**Основные виды деятельности обучающихся**	**Электронные образовательные ресурсы**
Безопасность общения (34 ч)	Вводное занятие (1 ч)	Выдвигать предположения о теме урока. Формулировать цели урока. Высказывать первые впечатления о понятии «Интернет». Пытаться аргументировать своё мнения, приводить примеров.	Заполняется по мере изучения содержания учебного предмета
	Общение в социальных сетях и мессенджерах (6ч.)	Социальные сети. История социальных сетей. Назначение социальных сетей и мессенджеров. Участвовать в беседе на тему «Что такое социальные сети?», воспроизводить знания и умения по данной теме. С кем безопасно общаться в интернете.	Заполняется по мере изучения содержания учебного предмета
	Распространение вредоносного кода (6ч)	Познакомиться с «вредоносными кодами», пониманием	Заполняется по мере изучения содержания

		его значения. Способы доставки вредоносных кодов. Исполняемые файлы и расширения вредоносных кодов. Правила защиты от вредоносных кодов.	учебного предмета
	Безопасный вход в аккаунты (4 ч)	Виды аутентификации. Настройки безопасности аккаунта. Понимать значение безопасности в при входе в аккаунты. Обдумывать, осмыслять, делать выводы, вносить индивидуальные предположения.	Заполняется по мере изучения содержания учебного предмета
	Настройки конфиденциальности в социальных сетях (6 ч)	Настройки приватности и конфиденциальности в разных социальных сетях. Учиться безопасно, пользоваться социальными сетями. Работать на чужом компьютере с точки зрения безопасности личного аккаунта.	Заполняется по мере изучения содержания учебного предмета
	Кибербуллинг (4 ч)	Определение кибербуллинга. Возможные причины кибербуллинга и как его избежать? Задуматься над своими действиями в социальных сетях. Как не стать жертвой кибербуллинга. Как помочь жертве кибербуллинга. Формировать умение высказывать свое мнение о культурном поведении в социальных сетях.	Заполняется по мере изучения содержания учебного предмета

	Фишинг(4ч.)	Популярные варианты распространения фишинга. Как отличить настоящие и фишинговые сайты. Как защититься от фишеров в социальных сетях и мессенджерах.	Заполняется по мере изучения содержания учебного предмета
	Проектная деятельность(3ч.)	Выполнение и защита индивидуальных и групповых проектов.	Заполняется по мере изучения содержания учебного предмета

8 КЛАСС

Тематический блок/раздел	**Основное содержание**	**Основные виды деятельности обучающихся**	**Электронные образовательные ресурсы**
Безопасность устройств **(34 ч)**	Вводное занятие (1 ч)	Изучить Программу курса «безопасное устройство» , формирования безопасного общения в социальных сетях. Правила безопасности в виртуальных контактах поддерживающего обстановку доброжелательности и радости общения, уважения друг к другу.	Заполняется по мере изучения содержания учебного предмета
	Виды вредоносных кодов (6 ч)	Что такое вредоносный код. Научиться их распознавать. Виды вредоносных кодов. Самостоятельно осуществлять поиск информации и использование	Заполняется по мере изучения содержания учебного предмета

		собранной социальной информации. Использовать приобретенные знания и умения в практической деятельности и повседневной жизни для: совершенствования собственной познавательной деятельности.	
	Методы защиты от вредоносных программ (7 ч)	Понимать значения вредоносных программ. Знать и уметь применять антивирусные программы и их характеристики. Правила защиты от вредоносных кодов.	Заполняется по мере изучения содержания учебного предмета
	Распространение вредоносного кода для мобильных устройств (3 ч)	Правила безопасности при установке приложений на мобильные устройства.	Заполняется по мере изучения содержания учебного предмета
	Публичные аккаунты (6ч.)	Научить правильно вести страничку в социальных сетях. Правила ведения публичных страниц. Понимать значение публичных страниц в социальных сетях.	Заполняется по мере изучения содержания учебного предмета
	Кибербуллинг (4 ч)	Определение кибербуллинга. Возможные причины кибербуллинга и как его избежать? Задуматься над своими действиями в социальных сетях. Как не стать жертвой кибербуллинга. Как помочь жертве	Заполняется по мере изучения содержания учебного предмета

		кибербуллинга. Формировать умение высказывать свое мнение о культурном поведении в социальных сетях.	
	Фишинг(4ч.)	Популярные варианты распространения фишинга. Как отличить настоящие и фишинговые сайты. Как защититься от фишеров в социальных сетях и мессенджерах.	Заполняется по мере изучения содержания учебного предмета
	Проектная деятельность (3 ч)	Выполнение и защита индивидуальных и групповых проектов	Заполняется по мере изучения содержания учебного предмета

9 КЛАСС

Тематический блок/раздел	Основное содержание	Основные виды деятельности обучающихся	Электронные образовательные ресурсы
Безопасность информации(34 ч)	Вводное занятие (1 ч)	Формировать правосознание и ответственность общения в социальных сетях. Знать о моральных и этических нормах взаимоотношений в обществе.	Заполняется по мере изучения содержания учебного предмета
	Правила безопасности в виртуальных контактах (3 ч)	Осознавать элементарные правила безопасности в виртуальных сетях.	Заполняется по мере изучения содержания учебного предмета
	Ложная информация в	Понимать сущность	Заполняется по

	Интернете (8 ч)	информации. Уметь отличать Фейковые новости. Поддельные страницы	мере изучения содержания учебного предмета
	Безопасность при использовании платежных карт в Интернете (8 ч)	Обладают представлениями о использовании платежных карт в Интернете. О правах и обязанностях при использовании платежных карт в Интернет.	Заполняется по мере изучения содержания учебного предмета
	Беспроводная технология связи (9 ч)	Уязвимости Wi-Fi-соединений. Понимать опасность и безопасность беспроводной связи. Уметь характеризовать основные социальные объекты, выделяя их существенные признаки, закономерности развития.	Заполняется по мере изучения содержания учебного предмета
	Резервное копирование данных(2ч.)	Уметь создавать резервные копий на различных устройствах.	Заполняется по мере изучения содержания учебного предмета
	Проектная деятельность (3 ч)	Участвовать в разработке учебных проектов.	Заполняется по мере изучения содержания учебного предмета

Календарно-тематическое планирование
7 класс. Всего 34 часа, 1 час в неделю.

№ урока п\п	Тема урока	Количество часов	Сроки	ОЭР
1.	Вводное занятие.	1	1 неделя	https://digital-

				likbez.datalesson.ru/videos/
2.	Общение в социальных сетях и мессенджерах.	1	2 неделя	https://digital-likbez.datalesson.ru
3.	С кем безопасно общаться в Интернете	1	3 неделя	https://www.ucheba.ru/project/websafety
4.	Пароли для аккаунтов социальных сетей	1	4 неделя	http://inf.kalga.edusite.ru/
5.	Безопасный вход в аккаунты	1	5 неделя	https://msk.tele2.ru/journal/article/20-rules-for-safety-internet
6.	Настройка конфендициальности в социальных сетях	1	6 неделя	https://24gadget.ru/1161071140-kak-zaschitit-konfidencialnost-grazhdan-rossii-v-socialnyh-setjah.html
7.	Публикация информации в социальных сетях.	1	7 неделя	https://www.cism-ms.ru/ostorozhno-seti-kakuyu-informatsiyu
8.	Методы защиты от вредоносных программ	1	8 неделя	https://www.google.com/search?
9.	Распространение вредоносных кодов для мобильных устройств		9 неделя	https://www.google.com/search?
10.	Способы доставки вредоносных кодов.	1	10 неделя	https://encyclopedia.kaspersky.ru/knowledge/how-malware-penetrates-systems/
11.	Исполняемые файлы и расширения вредоносных кодов	1	11 неделя	https://encyclopedia.kaspersky.ru/
12.	Способы выявления наличия вредоносных кодов на устройствах	1	12 неделя	https://encyclopedia.kaspersky.ru/knowledge/how
13.	Действия при обнаружении вредоносных кодов на устройствах.	1	13 неделя	https://encyclopedia.kaspersky.ru/knowledge/how-malware-penetrates-systems/
14.	Правила безопасности в виртуальных контактах	1	14 неделя	https://support.google.com

15.	Виды аутентификации	1	15 неделя	https://support.google.com/google-ads/answer/2375413?hl=ru
16.	Настройки безопасности аккаунта	1	16 неделя	https://www.tadviser.ru/index.php
17.	Работа на чужом компьютере с точки зрения безопасности личного аккаунта.	1	17 неделя	https://www.tadviser.ru
18.	Настройки приватности и конфиденциальности в разных социальных сетях.	1	18 неделя	https://ru.malwarebytes.com/malware/
19.	Приватность и конфидициальность в месседжерах.	1	19 неделя	https://ru.malwarebytes.com/malware/
20.	Публикация информации в социальных сетях	1	20 неделя	https://studfile.net/preview/4343195/page:7/
21.	Персональные данные	1	21 неделя	https://studfile.net/preview
22.	Публикация личной информации.	1	22 неделя	https://networkguru.ru/obzor-vozmozhnostey-raccoon-stealer/
23.	Публичные аккаунты	1	23 неделя	https://habr.com/ru/articles/748254/
24.	Определение кибербуллинга	1	24 неделя	https://powerdmarc.com/ru/what-is-malware/
25.	Возможные причины кибербуллинга и как его избежать?	1	25 неделя	https://powerdmarc.com
26.	Как не стать жертвой кибербуллинга	1	26 неделя	https://telefon-doveria.ru/kiberbulling-kak-pomoch-rebenku-v-sit
27.	Как помочь жертве кибербуллинга	1	27 неделя	https://telefon-doveria.rr
28.	Фишинг как мошеннический прием	1	28 неделя	https://ru.malwarebytes.com/phishing/
29.	Популярные варианты	1	29 неделя	https://ru.malwarebyt

	распространения фишинга.			es.com/
30.	Отличие настоящих и фишинговых сайтов	1	30 неделя	https://fincult.info/article/fishing-chto-eto-takoe-i-kak-ot-nego-zashchititsya/
31.	Как защититься от фишеров в социальных сетях и мессенджерах.	1	31 неделя	https://fincult.info/article/fishing-chto-eto-takoe
32.	Выбор темы проекта	1	32 неделя	https://infourok.ru/proekt-na-temu
33.	Этапы выполнения проекта	1	33 неделя	https://infourok.ru
34.	Выполнение и защита индивидуальных и групповых проектов	1	34 неделя	https://infourok.ru