МИНИСТЕРСТВО ПРОСВЕЩЕНИЯ РОССИЙСКОЙ ФЕДЕРАЦИИ
МБОУ "Школа №68" г.о. Самара

РАССМОТРЕНА	СОГЛАСОВАНА	УТВЕРЖДЕНА
Руководитель МО _____Донцова С.И. Протокол №1 от 28 августа 2025 г	Заместитель директора по УВР _____Юткина Н.М. Протокол №1 от 29 августа 2025 г	Директор МБОУ «Школы №68» г.о Самара _____Жидков А.А. Приказ №342 от 29 августа 2025г

ДОКУМЕНТ ПОДПИСАН
ЭЛЕКТРОННОЙ ПОДПИСЬЮ

Сертификат: 3197C49C36034CBE7353FEEDFE61D577
Владелец: Жидков Артём Алексеевич
Действителен: с 05.09.2024 до 29.11.2025

РАБОЧАЯ ПРОГРАММА

курса внеурочной деятельности

«Информационная безопасность»

Самара, 2025

Пояснительная записка

При составлении данной программы автором использованы следующие нормативно – правовые документы:

- Федеральный государственный образовательный стандарт основного общего образования;
- Основная образовательная программа основного общего образования МБОУ Школа №68 г.о. Самара

Программа составлена на основе:

М.С. Наместников Информационная безопасность, или На расстоянии одного вируса. 7-9 класс: учеб. Пособие для общеобразовательных организаций/ Просвещение, 2019

Актуальность

Развитие глобального процесса информатизации общества, охватывающего все развитые и многие развивающиеся страны мира, приводит к формированию новой информационной среды, информационного уклада и профессиональной деятельности. Однако при этом пропорционально возрастает уязвимость личных, общественных и государственных информационных ресурсов со стороны негативного воздействия средств информационно-коммуникационных технологий.

Таким образом, мировое сообщество стоит перед глобальной социотехнической проблемой – проблемой обеспечения информационной безопасности.

Решение проблемы безопасности вообще и информационной безопасности в частности невозможно без достаточного количества как высококвалифицированных профессионалов, так квалифицированных пользователей, компетентных в сфере защиты информации.

Данный курс преследует следующие **цели**:

- Овладение учащимися умениями: профилактики, защиты программного обеспечения; обнаружения и удаления компьютерных вирусов; защиты информации в автоматизированных системах обработки данных, в глобальной сети Интернет.
- Приобретение учащимися опыта по предупреждению и нейтрализации негативного воздействия информационных угроз на людей и программно - технические комплексы; опыта информационной деятельности в сферах обеспечения защиты информации, актуальных на рынке труда.
- Приобретения учащимися опыта создания, редактирования, оформления, сохранения, передачи информационных объектов различного типа с помощью современных программных средств; коллективной реализации информационных проектов, преодоления трудностей в процессе проектирования, разработки и реализации учебных проектов.

Перед данным элективным курсом ставятся следующие **задачи**:

- освоение учащимися знаний, относящихся к основам обеспечения информационной безопасности, и их систематизация;
- изучение учащимися мер законодательного, административного, процедурного и программно-технического уровней при работе на вычислительной технике и в системах связи;
- повышение интереса учащихся к изучению информатики;
- приобретение учащимися навыков самостоятельной работы с учебной, научно -популярной литературой и материалами сети Интернет;
- развитие у учащихся способностей к исследовательской деятельности;
- воспитание у учащихся культуры в области применения ИКТ в различных
- сферах современной жизни;
- воспитание у учащихся чувства ответственности за результаты своего труда, используемые другими людьми;
- воспитание у учащихся умения планировать, работать в коллективе;
- воспитание у учащихся нравственных качеств, негативного отношения к нарушителям информационной безопасности;
- воспитание у учащихся установки на позитивную социальную деятельность в информационном обществе, недопустимость действий, нарушающих правовые и этические нормы работы с информацией.

Планируемые результаты освоения курса:

Личностные результаты

Основными личностными результатами, формируемыми при изучении программирования, являются:

- ответственное отношение к учению, готовность к саморазвитию и самообразованию;
- осознанный выбор и построение дальнейшей индивидуальной траектории образования;
- умение контролировать процесс и результат учебной деятельности;
- критичность мышления, инициатива, активность при решении алгоритмических задач.

Метапредметные результаты

- Основными метапредметными результатами, формируемыми при изучении информатики в основной школе, являются:
- умение самостоятельно определять цели своего обучения, развивать

мотивы и интересы своей познавательной деятельности;

- умение соотносить свои действия с планируемыми результатами;
- умение определять понятия, обобщать, устанавливать аналогии, классифицировать;
- развивать компетенции в области использования информационно-коммуникационных технологий;
- умение находить информацию в различных источниках;
- умение выдвигать гипотезы;
- понимать сущности алгоритмических предписаний;
- устанавливать причинно-следственные связи, проводить доказательные рассуждения;
- умение иллюстрировать изученные понятия и свойства алгоритмов и программ.

Предметные результаты

- осознание значения алгоритмизации и программирования для повседневной жизни;
- развитие умений работать с математическим текстом;
- выражать свои мысли с применением терминологии компьютерной математики и теоретических основ информатики и программирования;
- владение базовым понятийным аппаратом по основным разделам содержания;
- практически значимые умения и навыки алгоритмизации и программирования, их применение к решению математических и алгоритмических задач

Содержание курса внеурочной деятельности

Тема 1 Безопасное общение

Общение в социальных сетях и мессенджерах. С кем безопасно общаться в Интернете. Пароли для аккаунтов социальных сетей. Вход в аккаунт социальных сетей. Настройки конфиденциальности в социальных сетях и мессенджерах. Публикация информации в социальных сетях. Кибербуллинг. Публичные аккаунты. Фишинг.

Тема № 2: Безопасность устройств

Что такое вредоносный код. Распространение вредоносного кода. Методы защиты от вредоносных программ. Распространение вредоносного кода для

мобильных устройств.

Тема № 3: Безопасность информации

Социальная инженерия: распознать и избежать. Ложная информация в Интернете. Безопасность при использовании платёжных карт в Интернете. Беспроводная технология связи.

Тематическое планирование

№	Наименование тем занятий, разделов	Количество часов отведенных на теорию	Количество часов отведенных на практику
Тема № 1: Безопасное общение			
1	Общение в социальных сетях и мессенджерах	1	1
2	С кем безопасно общаться в Интернете	1	1
3	Пароли для аккаунтов социальных сетей	1	1
4	Вход в аккаунт социальных сетей	1	1
5	Настройки конфиденциальности в социальных сетях и мессенджерах	1	1
6	Публикация информации в социальных сетях	1	1
7	Кибербуллинг	1	1
8	Публичные аккаунты	1	1
9	Фишинг	1	1
Тема № 2: Безопасность устройств			
10	Что такое вредоносный код	1	1
11	Распространение вредоносного кода	1	1
12	Методы защиты от вредоносных программ	1	1
13	Распространение вредоносного кода для мобильных устройств	1	1

Тема № 3: Безопасность информации			
14	Социальная инженерия: распознать и избежать	1	1
15	Ложная информация в Интернете	1	1
16	Безопасность при использовании платёжных карт в Интернете	1	1
17	Беспроводная технология связи	1	1
	Итого:	**17** **50 %**	17 **50%**

Работа с родителями

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.

Тематическое планирование учебного курса (для родителей).

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. Обеспечение эмоционально-психологического периметра безопасности в соответствии с возрастными особенностями ребенка. 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. Контентные риски. Настройка и безопасное использование смартфона или планшета. Семейный доступ.

Тема 8. Пособия и обучающие программы по формированию навыков цифровой гигиены.