МИНИСТЕРСТВО ПРОСВЕЩЕНИЯ РОССИЙСКОЙ ФЕДЕРАЦИИ
Муниципальное бюджетное общеобразовательное учреждение
«Средняя Общеобразовательная школа № 16»
МБОУ «СОШ № 16»

РАССМОТРЕНО	СОГЛАСОВАНО	УТВЕРЖДЕНО
на заседании МО	на методическом совете	Директор МБОУ "СОШ № 16"
_____	_____	_____
Руководитель МО Улаханова С.Н	Заместитель директора Платонова Г.В	Ефимова М.В
Протокол № 1 от «02» 09 2024 г.	Протокол № от «02» 09 2024 г.	Приказ № 40-05 от «02» 09 2024 г.

РАБОЧАЯ ПРОГРАММА
По внеурочной деятельности
«IT-волонтеры»
для обучающихся 5 – 9 классов

г.Ангарск, 2024

ПОЯСНИТЕЛЬНАЯ ЗАПИСКА

Рабочая программа внеурочной деятельности «IT-волонтеры» разработана в связи с возросшей потребностью обеспечения информационной безопасности детей при организации урочной и внеурочной деятельности. Рабочая программа курса «IT-волонтеры» для обучающихся 5-9 классов составлена на основе следующих документов:

- Федеральный государственный образовательный стандарт основного общего образования / Мин-во образования и науки РФ. -2-е изд. -М.: просвещение

-Федеральный закон "Об образовании в Российской Федерации" от 29.12.2012 № 273-Ф

- Стратегия национальной безопасности Российской Федерации, Указ Президента Российской Федерации от 2 июля 2021 г. № 400 «О Стратегии национальной безопасности Российской Федерации».

-Приказ Министерства просвещения Российской Федерации от 31.05.2021 № 287 «Об утверждении федерального государственного образовательного стандарта основного общего образования» (Зарегистрирован Минюстом России 05.07.2021 № 64101).

-Приказ Министерства просвещения Российской Федерации от 18.07.2022 № 568 «О внесении изменений в федеральный государственный образовательный стандарт основного общего образования» (Зарегистрирован Минюстом России 17.08.2022 № 69675).

-.Приказ Министерства просвещения Российской Федерации от 31.05.2021 № 287 «Об утверждении федерального государственного образовательного стандарта основного общего образования» (Зарегистрирован Минюстом России 05.07.2021 № 64101).

-.Приказ Министерства просвещения Российской Федерации от 18.07.2022 № 568 «О внесении изменений в федеральный государственный образовательный стандарт основного общего образования» (Зарегистрирован Минюстом России 17.08.2022 № 69675).

- Приказ Министерства просвещения Российской Федерации от 18.05.2023 № 370 «Об утверждении федеральной образовательной программы основного общего образования» (Зарегистрирован Минюстом России 12.07.2023 № 74223).

Рабочая программа внеурочной деятельности для обучающихся 5 - 9 классов (уровень основного общего образования) составлена на основе основной образовательной программы основного общего образования МБОУ «СОШ №16» с учётом требований к предметным результатам освоения образовательной программы.

Программа разработана с учетом требований законов Российской Федерации: «Об образовании в Российской Федерации», «О защите детей от информации, причиняющей вред их здоровью и развитию» и «Санитарно - эпидемиологических требований к условиям и организации обучения в общеобразовательных учреждениях» и "Санитарноэпидемиологических требований к устройству, содержанию и организации режима работы образовательных организаций дополнительного образования детей".

Курс «IT-волонтеры» 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.

Основными целями изучения курса «IT-волонтеры» 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 информационнотелекоммуникационной 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.

Программа составлена на основе курса «Основы кибербезопасности» для общеобразовательных организаций авторов Тонких И.М.,

Согласно учебному плану МБОУ «СОШ №16» на изучение курса внеурочной деятельности «IT-волонтеры» выделено по 1 часу в неделю в 5,6,7,8,9 классах, всего по 34 часа в год.

I. Планируемые предметные результаты освоения учебного предмета

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

II. Содержание курса

Содержание программы учебного курса соответствует темам основной образовательной программы основного общего образования по учебным предметам «Информатика» и «Основы безопасности жизнедеятельности», 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».

5,6, класс

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 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. 3 часа. Повторение. 3 часа.**

7-8 класс

Модуль 1. Медиа и человек как потребитель информации

Медиа как источник информации. Функции медиа. Виды медиа. Медиасреда современного человека. Интернет как составляющая медиасреды.

Информационные угрозы. Агрессия в киберпространстве (троллинг, хейтинг, кибersталкинг, грифинг, кибербуллинг, кибергрумминг), способы защиты от агрессии.

Распознавание фейковой информации на основе критического анализа. Виды противоправного контента в цифровом пространстве (экстремистский, террористический, наркотический, суицидальный). Что делать, если столкнулся с противоправным контентом или вербовщиком?

Мошенничество в сети Интернет. Защита от различных видов цифрового мошенничества. Создание надежного пароля.

Модуль 2. Медиа и человек как производитель информации.

Интернет-отношения, права и обязанности пользователей цифрового пространства: соблюдение законов и правил в онлайн-взаимодействии, защита персональных данных, авторское право в интернете. Культура сетевого общения.

Общение в соцсетях и мессенджерах. Защита от угроз в соцсетях.

Контент, виды контента. Создание собственного безопасного контента. Медиаграмотность в цифровом мире.

В первом модуле «Медиа и человек как потребитель информации» раскрываются основные особенности медиасреды и важнейшие приемы безопасной работы в ней. Особое внимание уделяется сети Интернет. Рассматриваются положительные и отрицательные стороны ее использования. Основной частью содержания данного модуля является рассмотрение опасностей и рисков, которые могут встретиться в сети Интернет (агрессия, фейковая информация, противоправный контент, мошенничество), способов защиты от них.

Во втором модуле «Медиа и человек как производитель информации» рассматриваются правовые основы безопасного поведения в цифровом пространстве, общение в социальных сетях и мессенджерах. Акцентируется важность соблюдения правовых, нравственных и моральных норм в ходе онлайн-взаимодействия. Уделяется внимание практической составляющей: созданию контента по конкретной ситуации, обеспечению безопасности собственного контента.

III. Календарно-тематическое планирование

5,6 класс

№ п/п	Тема	Дата
	Тема 1. «Безопасность общения»	
1	Общение в социальных сетях и мессенджерах	
2	С кем безопасно общаться в интернете	
3	Пароли для аккаунтов социальных сетей	
4	Безопасный вход в аккаунты	
5	Настройки конфиденциальности в социальных сетях	
6	Публикация информации в социальных сетях	
7	Кибербуллинг	
8	Публичные аккаунты	
9	Фишинг	
10	Фишинг	
11	Выполнение индивидуальных и групповых проектов	
12	Выполнение индивидуальных и групповых проектов	
13	Выполнение индивидуальных и групповых проектов	
	Тема 2. «Безопасность устройств»	
14	Что такое вредоносный код	
15	Распространение вредоносного кода	
16	Методы защиты от вредоносных программ	
17	Методы защиты от вредоносных программ	

18	Распространение вредоносного кода для мобильных устройств	
19	Выполнение и защита индивидуальных и групповых проектов	
20	Выполнение и защита индивидуальных и групповых проектов	
21	Выполнение и защита индивидуальных и групповых проектов	
	Тема 3. «Безопасность информации»	
22	Социальная инженерия: распознать и избежать	
23	Ложная информация в Интернете	
24	Безопасность при использовании платежных карт в Интернете	
25	Беспроводная технология связи	
26	Резервное копирование данных	
27	Основы государственной политики в области формирования культуры информационной безопасности	
28	Основы государственной политики в области формирования культуры информационной безопасности	
29	Выполнение и защита индивидуальных и групповых проектов	
30	Выполнение и защита индивидуальных и групповых проектов	
31	Выполнение и защита индивидуальных и групповых проектов	
32	Повторение	
33	Повторение	
34	Повторение	
	Итого	**34**

7 класс

№ п/п	**Тема**	**Дата**
	Модуль 1. Медиа и человек как потребитель информации	
1-2	Социальные сети	
3-4	Социальные медиа и коммуникаторы	
5-6	Медиа как источник информации. Виды медиа: от СМИ до видеоигр и стримов.	
7-8	Какой не должна быть страничка в соц.сетях	
9-10	Кибермоббинг.	
11-12	Информационные угрозы в интернете и защита от них: агрессия.	
13-14	Информационные угрозы в интернете и защита от них: фейки и противоправный контент.	
15-16	Как отличить фейки от оригинала	
17-18	Информационные угрозы в интернете и защита от них: мошенничество.	
	Модуль 2. Медиа и человек как производитель информации	
19-20	Правила общения в интернете.	
21-22	Новостная грамотность. Оценка достоверности	

23-24	Общение в мессенджерах.	
25-26	Создаем интересный и безопасный контент.	
27-28	Почтовые сервисы. Создание и настройка правил.	
29-30	Родительский контроль. Белый и черный список	
31-32	Электронные финансы. Облачные хранилища	
33-34	Повторение	
	Итого	**34**

8 класс

№ п/п	**Тема**	**Дата**
	Модуль 1. Безопасность в виртуальном мире	
1-2	Как защитить персональные данные? Мой аккаунт- моя крепость.	
3-4	Как оградить и обезопасить свое медиапространство.	
5-6	Общение в соцсетях и мессенджерах. Как понять, что аккаунт фейковый?	
7-8	Агрессия в социальных сетях и способы защиты.	
9-10	Опасности, с которыми дети могут столкнуться в сети Интернет. Организация правильного поиска необходимой информации в сети Интернет и СМИ.	
11-12	Кибербулинг. Как привлечь к ответственности за кибербулинг.	
13-14	Доксинг в интернете. Противостояние угрозам из Интернета.	
15-16	Всегда ли можно доверять информации в интернете?	
17-18	Инструкции по безопасному общению в чатах. Интернетэтика поведения в Интернете.	
19-20	Феномен «Интернет-зависимости». Профилактика Интернет-зависимости.	
21-22	Технологии и средства защиты информации от противоправных посягательств в сети Интернет, мобильной (сотовой) связи и СМИ.	
23-24	Уровни и меры по защите информации. Меры безопасности при работе с электронной почтой	
25-26	Основы безопасности при использовании мобильной (сотовой) связи. Виды мошенничества в мобильной связи. Меры предосторожности и безопасности при использовании сотовой (мобильной) связи.	
27-28	Обзор и классификация компьютерных вирусов. Способы распространения вирусов. История вредоносных программ. Вирусная терминология.	
29-30	Самые распространенные вирусы. Цикл функционирования вирусов.	
31-32	Антивирусное программное обеспечение и антишпионские программы. Методы борьбы с вирусами.	

33-34	Меры защиты от проникновения и распространения вирусов.	
	Итого	**34**

9 класс

№ п/п	Тема	Дата
	Модуль 1. Информационные угрозы . Как противостоять?	
1-2	Противоправный контент в сети Интернет. Как организации становятся экстремистскими и террористическим	
3-4	Особенности экстремизма в молодежной среде. Мифы о наркотиках.	
5-6	Как не стать жертвой интернет- мошенника. Как обезопасить аккаунт от взлома.	
7-8	Информационный лонгрид «Тренды онлайн- мошенничества и способы себя защитить.	
9-10	Как не попасть на крючок мошенников? Что такое фишинг и как с ним бороться. Что такое овершеринг.	
11-12	Как критическое мышление позволяет бороться с фейками. Как проверять информацию и не стать жертвой фейков.	
13-14	Вымысел в искусстве.Нужны ли сказки для взрослых?	
15-16	Музыка и эмоциональные манипуляции в кино. Как повлиять на людей за 50 сек?	
17-18	Фейк и фантазия .Как распознать фейки?	
19-20	Медиаграмотность в цифровом мире.10 цифровых привычек.	
21-22	Мини-квиз «Безопасный интернет». Как обезопасить себя от цифровых преступников.	
23-24	Кто производит фото и видеофейки	
25-26	Рассылки в мессенджирах	
27-28	Что такое цифровой след и как его чистить.	
29-30	Информация и ее признаки. Искажение признаков информации и его последствия.	
31-32	Механизм искажения информации. Факторы влияния на информацию	
33-34	Повторение	
	Итого	**34**

Список используемой литературы

1. Давлетов, З.Х. Основы современной информатики: Учебное пособие / З.Х. Давлетов. - СПб.: Лань КПТ, 2016. - 256 с. 2. Кудинов, Ю.И. Основы современной информатики: Учебное пособие / Ю.И. Кудинов, Ф.Ф. Пащенко. - СПб.: Лань, 2018. - 256 с. 3. Чепурнова, Н.М. Правовые основы информатики: Учебное пособие / Н.М. Чепурнова, Л.Л. Ефимова. - М.: Юнити, 2015. - 295 с. 4. Чепурнова, Н.М. Правовые основы информатики. Учебное пособие / Н.М. Чепурнова, Л.Л. Ефимова. - М.: Юнити, 2017. - 184 с.