

МИНИСТЕРСТВО ПРОСВЕЩЕНИЯ РОССИЙСКОЙ ФЕДЕРАЦИИ

**МУНИЦИПАЛЬНОЕ АВТОНОМНОЕ ОБЩЕОБРАЗОВАТЕЛЬНОЕ
УЧРЕЖДЕНИЕ «СРЕДНЯЯ ОБЩЕОБРАЗОВАТЕЛЬНАЯ ШКОЛА № 2»**

Рассмотрена
и рекомендована к утверждению
на заседании методического совета
протокол от 30.08.2023 № 1

Утверждено
Директор школы
Е.Д.Выжимов
Приказ от 31.08.2023 №90

РАБОЧАЯ ПРОГРАММА

учебного предмета «Кибербезопасность»

для обучающихся 5–8 классов

Тамбов 2024

ПОЯСНИТЕЛЬНАЯ ЗАПИСКА

Программа по кибербезопасности на уровне основного общего образования составлена на основе требований к результатам освоения основной образовательной программы основного общего образования, представленных в ФГОС ООО, а также федеральной рабочей программы воспитания.

Программа по кибербезопасности даёт представление о целях, общей стратегии обучения, воспитания и развития, обучающихся средствами кибербезопасности на базовом уровне, устанавливает обязательное предметное содержание, предусматривает его структурирование по разделам и темам.

Программа по кибербезопасности определяет количественные и качественные характеристики учебного материала для каждого года изучения, в том числе для содержательного наполнения разного вида контроля (промежуточной аттестации обучающихся, всероссийских проверочных работ, государственной итоговой аттестации).

Программа по кибербезопасности является основой для составления авторских учебных программ, тематического планирования курса учителем.

Целями изучения кибербезопасности на уровне основного общего образования являются:

формирование цифровой компетентности школьников и расширение возможностей полезного, критичного, ответственного и безопасного использования Интернета;

формирование основ мировоззрения, соответствующего современному уровню развития науки кибербезопасности, достижениям научно-технического прогресса и общественной практики, за счёт развития представлений об информации как о важнейшем стратегическом ресурсе развития личности, государства, общества, понимания роли информационных процессов, информационных ресурсов и информационных технологий в условиях цифровой трансформации многих сфер жизни современного общества;

обеспечение условий, способствующих развитию алгоритмического мышления как необходимого условия профессиональной деятельности в современном информационном обществе, предполагающего способность обучающегося разбивать сложные задачи на более простые подзадачи, сравнивать новые задачи с задачами, решёнными ранее, определять шаги для достижения результата и так далее;

формирование и развитие компетенций обучающихся в области использования информационно-коммуникационных технологий, в том числе знаний, умений и навыков работы с информацией, программирования,

коммуникации в современных цифровых средах в условиях обеспечения информационной безопасности личности обучающегося;

воспитание ответственного и избирательного отношения к информации с учётом правовых и этических аспектов её распространения, стремления к продолжению образования в области информационных технологий и созидательной деятельности с применением средств информационных технологий.

Кибербезопасность в основном общем образовании отражает:

сущность кибербезопасности как научной дисциплины, изучающей закономерности протекания и возможности автоматизации информационных процессов в различных системах;

основные области применения кибербезопасности, прежде всего информационные технологии, управление и социальную сферу;

междисциплинарный характер кибербезопасности и информационной деятельности.

Изучение кибербезопасности оказывает существенное влияние на формирование мировоззрения обучающегося, его жизненную позицию, закладывает основы понимания принципов функционирования и использования информационных технологий как необходимого инструмента практически любой деятельности и одного из наиболее значимых технологических достижений современной цивилизации. Многие предметные знания и способы деятельности, освоенные обучающимися при изучении кибербезопасности, находят применение как в рамках образовательного процесса при изучении других предметных областей, так и в иных жизненных ситуациях, становятся значимыми для формирования качеств личности, то есть ориентированы на формирование метапредметных и личностных результатов обучения.

Основные задачи учебного предмета «Кибербезопасность» – сформировать у обучающихся:

диапазон возможностей, связанных с использованием цифровых технологий;

осознание влияния, которое цифровые технологии оказывают на их образ жизни;

представления о возможностях Интернета как источника информации, инструмента коммуникации и потребления;

устойчивых стратегий своевременного распознавания онлайн-рисков и безопасного поведения при столкновении с ними, сформировать навыки успешного разрешения проблемных ситуаций в Сети, защиты своих персональных данных и управления ими;

адекватного образа цифровых технологий, предполагающего, с одной стороны, понимание их позитивной роли в развитии человеческой цивилиза-

ции, а с другой — критическую оценку влияния цифровых технологий на разные стороны жизнедеятельности человека;

критического мышления, творческого мышления и креативности, способности к рефлексии, навыков сотрудничества.

Цели и задачи изучения кибербезопасности на уровне основного общего образования определяют структуру основного содержания учебного предмета в виде следующих семи тематических разделов:

Цифровой мир и интернет-зависимость.

Техносфера и технические риски.

Информация и контентные риски.

Общение и коммуникационные риски.

Цифровая экономика и потребительские риски.

Персональные данные.

Цифровое будущее.

На изучение кибербезопасности отводится 136 часов: в 5 классе – 34 часа (1 час в неделю), в 6 классе – 34 часа (1 час в неделю), в 7 классе – 34 часа (1 час в неделю), в 8 классе – 34 часа (1 час в неделю)

5 КЛАСС

Зачем нам нужен Интернет

Создание современного Интернета. Тим Бернерс Ли. Всемирная паутина. Новые возможности Интернета в осуществлении традиционных социально-культурных практик. Типы интернет-пользователей. Проблема интернет-зависимости. Сбалансированный распорядок дня.

Как устроен Интернет

Компьютерная программа. Первая в мире компьютерная программа. Браузер. Программное обеспечение, софт. Профессия программист. Техносфера. Виды цифровых устройств. Три кита Интернета: «железо», софт, сети. Компьютерные вирусы. Правила защиты цифрового устройства от компьютерных вирусов.

Какая бывает информация

Что такое информация. Цифровая информация. Контент. Ценность информации. Каналы восприятия информации. Возможности использования каналов восприятия информации в Интернете. Единицы измерения цифровой информации. Формы представления цифровой информации в Интернете.

Как работает поиск в Интернете

Поиск информации. Поисковая система. Полезные ресурсы в Интернете. Контентные риски: столкновение с неприятным он-лайн-контентом. Способы защиты от контентных рисков: настройки безопасного поиска и кнопка «пожаловаться на контент».

Как люди общаются в Интернете

Сервисы для общения в Интернете. Возможности общения в Интернете. Рэй Томлинсон. Первое в мире электронное сообщение. Плюсы и минусы цифрового общения. Правила онлайн-общения.

Как совершать покупки в Интернете

Цифровая экономика. Реальные и виртуальные товары. Первый в мире интернет-магазин. Критерии надёжности интернет-магазина. Плюсы и минусы интернет-магазинов. Баннеры, реклама. Правила безопасности при совершении покупок в Интернете.

Что такое персональные данные

Общедоступная и персональная информация. Персональные данные. Виды персональных данных.

Какие следы мы оставляем в Интернете

Виды персональных данных, выкладываемых в открытый доступ. Риски размещения персональной информации в открытом доступе. Настройки приватности.

Урок в школе будущего

Современные технологии, используемые в процессе обучения.

6 КЛАСС

Мы в цифровом мире

Информационные революции, история средств связи. Функции и роль Интернета в повседневной жизни. Возможности и риски, связанные с Интернетом. Интернет-зависимость. Варианты организации свободного времени без использования гаджетов и Интернета.

Почему важны пароли в Интернете

История паролей. Всемирный день пароля. Аккаунт, логин, пароль, аутентификация, авторизация. Способы защиты аккаунта (пароль, отпечаток пальца, одноразовый код, USB-ключ, двухфакторная аутентификация). Правила безопасности при защите аккаунта (создание, использование и хранение надёжных паролей). Алгоритмы создания паролей.

Полезные интернет-ресурсы

Виды информационных ресурсов. Что такое контент. Контент в Интернете. Полезные онлайн-ресурсы. Цифровые образовательные ресурсы. Контентные риски. Способы защиты от нежелательного контента в Интернете.

Как искать и распознавать правдивую информацию

Потребность в информации. Информационная социализация. Инструменты для быстрого поиска в Интернете. Достоверность информации. Что такое фейк. Пост и репост в социальной сети. Способы определения достоверности информации.

Как общаться в Интернете

Самопрезентация. Особенности самопрезентации в Интернете. Общение в Интернете. История смайлика. Преимущества и недостатки общения в Интернете. Вербальное и невербальное общение. Эмодзи. Особенности передачи и восприятия информации, выраженной при помощи смайликов и эмодзи и при помощи текста. Уместное и неуместное использование смайликов и эмодзи в онлайн-общении.

Как избежать конфликтов в Интернете

Агрессивное и неагрессивное общение. Причины агрессии в Интернете. Правила безопасности при общении в Интернете. Троллинг. Стратегии поведения при столкновении с троллингом. Пути решения проблемы агрессии в Интернете. Возможности бесконфликтного общения в Интернете. Способы поддержки человека, столкнувшегося с агрессией в Интернете. Флешмобы. Правила бесконфликтного общения в Интернете.

Как не попасться на удочку онлайн-мошенникам

Цифровая экономика. Преимущества и риски покупок онлайн. Интернет-мошенничество. Фишинг. Виды интернет-мошенничества и их последствия. Спам. Способы защиты от спама. СМС-мошенничество. Способы защиты от интернет- и СМС-мошенничества.

Что такое персональные данные

Персональные данные. Публичная и персональная информация. Идентификатор личности. Виды персональных данных.

Что нужно знать о цифровых следах

Цифровой след. Понятие приватности. Настройки приватности в цифровых устройствах. Виды кодов (линейный штрихкод и QR-код). Источники частных сведений о человеке. Рекомендации по управлению приватностью в Интернете.

Дома будущего

Новшества в архитектуре и строительстве, связанные с цифровыми технологиями. Применение цифровых технологий в быту.

7 КЛАСС

Как не заблудиться в Интернете

Место Интернета в жизни современного человека. Домен и доменное имя. Виды доменов. Требования к доменным именам. Проблема интернет-зависимости. Всплывающие уведомления. Профилактика чрезмерной увлечённости Интернетом.

Как безопасно подключаться к Интернету

Способы подключения к Интернету. Проводное и беспроводное соединение. Правила безопасности при беспроводном подключении к Интернету. Правила и алгоритмы составления надёжного пароля.

Как искать полезную информацию в Интернете

Потребность в информации как одна из базовых потребностей человека. Контент сайта. Механизм работы поисковых систем. Возможности и правила поиска в поисковых системах Google и Яндекс. Функция «поиск по картинке». Информационная перегрузка.

Почему нужно проверять информацию в Интернете

Достоверная и недостоверная информация. Фейковые новости. Признаки недостоверной, фейковой информации.

Человек в Интернете: реальный или виртуальный?

Способы общения в Интернете. Форумы, чаты, мессенджеры. «Друзья» в социальных сетях и Интернете. Аватар — «лицо» человека в Интернете. Механизм формирования образа человека в Интернете. Риски общения с незнакомцами в Интернете. Правила безопасного общения с интернет-

друзьями.

Как противостоять агрессии в Интернете

Агрессия и конфликты в Интернете. Троллинг. Действия по профилактике агрессивного поведения в Интернете. Действия при столкновении с агрессией в Интернете.

Как безопасно совершать покупки в Интернете

Цифровая экономика. Покупки в Интернете. Риски онлайн-шопинга. Правила безопасности при совершении покупок онлайн.

Как персональные данные оказываются в Сети

Персональные данные. Конфиденциальность. Цифровые следы. Способы попадания персональных данных в Сеть. Куки-файлы. Правила защиты персональных данных. Режим инкогнито. Три кита защиты персональных данных: надёжные пароли, настройки приватности, управление персональными данными.

Для чего нужно управлять персональными данными

Значимость персональных данных. Способы управления персональными данными в Интернете. Рекомендации по предотвращению кражи персональных данных.

Цифровой мир будущего

Интернет вещей. Цифровые технологии и предметы повседневного пользования.

8 КЛАСС

Другая реальность — дополненная и виртуальная

Виртуальная реальность. Дополненная реальность. История развития технологий виртуальной и дополненной реальности. Применение виртуальной и дополненной реальности в разных сферах жизни. Видеоигры. Зависимость от видеоигр. Профилактика зависимости от видеоигр.

Защита от вредоносных программ

Вредоносные программы: мифы и реальность. Компьютерный вирус. Виды вредоносных программ. Троянская программа. Способы защиты от технических рисков.

Как стать мастером поиска в Интернете

Команды быстрого поиска в Интернете. Возможности строки поиска для решения математических задач. Нежелательный контент. Способы борьбы с нежелательным контентом.

Фейки в Интернете: как их распознать

Фейковые новости. Фактчекинг. Признаки фейковых новостей. Способы

определения фейковых видео и фотографий. База знаний Wolfram Alpha. Критерии оценки достоверности информации.

Репутация в Интернете: как её сохранить

Репутация и самопрезентация в Интернете и офлайн. Риски, сопряжённые с самопрезентацией в Интернете. Негативное и положительное влияние поведения в Интернете на репутацию в жизни офлайн. Управление репутацией.

Агрессия в Сети: способы предотвращения

Проявление агрессии в Интернете. Влияние столкновения с агрессией в Сети на пользователей. Профилактика агрессии в Сети. Технические средства защиты от агрессии в Сети. Социальная реклама. Правила безопасного общения в Интернете.

Электронные платежи: правила безопасности

История денег. Банковские онлайн-операции. Интернет-платежи. Цифровая экономика. Платёжные карты. Виртуальные деньги. Криптовалюты. Риски при осуществлении интернет-платежей. Правила безопасности при осуществлении покупок в Интернете.

Персональные данные в Сети: как их защитить

Государственный контроль над защитой персональных данных, Роскомнадзор. Сайт «Персональные данные. дети». Федеральный закон «О персональных данных», персональные данные, оператор персональных данных, обработка персональных данных. Виды персональных данных. Признаки надёжного пароля. Способы создания надёжного пароля. Как пароли попадают к мошенникам. Правила хранения и защиты паролей.

Оберегаем личное пространство в Интернете

Приватность. Личное пространство. Личные границы. Зоны общения. Распределение персональных данных по зонам общения. Шкала «открытости-закрытости». Тест на степень открытости в Интернете. Настройки приватности в социальных сетях. Рекомендации по настройкам приватности в социальных сетях.

Профессии будущего

Цифровые технологии и профессии. Изменения в мире профессий. Новые профессии, связанные с цифровыми технологиями.

ПЛАНИРУЕМЫЕ РЕЗУЛЬТАТЫ ОСВОЕНИЯ ПРОГРАММЫ ПО

ИНФОРМАТИКЕ НА УРОВНЕ ОСНОВНОГО ОБЩЕГО ОБРАЗОВАНИЯ

Изучение информатики на уровне основного общего образования направлено на достижение обучающимися личностных, метапредметных и предметных результатов освоения содержания учебного предмета.

ЛИЧНОСТНЫЕ РЕЗУЛЬТАТЫ

Личностные результаты имеют направленность на решение задач воспитания, развития и социализации обучающихся средствами учебного предмета.

В результате изучения информатики на уровне основного общего образования у обучающегося будут сформированы следующие личностные результаты в части:

1) патриотического воспитания:

ценностное отношение к отечественному культурному, историческому и научному наследию, понимание значения информатики как науки в жизни современного общества, владение достоверной информацией о передовых мировых и отечественных достижениях в области информатики и информационных технологий, заинтересованность в научных знаниях о цифровой трансформации современного общества;

2) духовно-нравственного воспитания:

ориентация на моральные ценности и нормы в ситуациях нравственного выбора, готовность оценивать своё поведение и поступки, а также поведение и поступки других людей с позиции нравственных и правовых норм с учётом осознания последствий поступков, активное неприятие асоциальных поступков, в том числе в Интернете;

3) гражданского воспитания:

представление о социальных нормах и правилах межличностных отношений в коллективе, в том числе в социальных сообществах, соблюдение правил безопасности, в том числе навыков безопасного поведения в интернет-среде, готовность к разнообразной совместной деятельности при выполнении учебных, познавательных задач, создании учебных проектов, стремление к взаимопониманию и взаимопомощи в процессе этой учебной деятельности, готовность оценивать своё поведение и поступки своих товарищей с позиции нравственных и правовых норм с учётом осознания последствий поступков;

4) ценностей научного познания:

сформированность мировоззренческих представлений об информации, информационных процессах и информационных технологиях, соответствующих современному уровню развития науки и общественной практики и составляющих базовую основу для понимания сущности научной картины мира;

интерес к обучению и познанию, любознательность, готовность и способность к самообразованию, осознанному выбору направленности и уровня обучения в дальнейшем;

овладение основными навыками исследовательской деятельности, установка на осмысление опыта, наблюдений, поступков и стремление совершенствовать пути достижения индивидуального и коллективного благополучия;

сформированность информационной культуры, в том числе навыков самостоятельной работы с учебными текстами, справочной литературой, разнообразными средствами информационных технологий, а также умения самостоятельно определять цели своего обучения, ставить и формулировать для себя новые задачи в учёбе и познавательной деятельности, развивать мотивы и интересы своей познавательной деятельности;

5) формирования культуры здоровья:

осознание ценности жизни, ответственное отношение к своему здоровью, установка на здоровый образ жизни, в том числе и за счёт освоения и соблюдения требований безопасной эксплуатации средств информационных и коммуникационных технологий;

б) трудового воспитания:

интерес к практическому изучению профессий и труда в сферах профессиональной деятельности, связанных с информатикой, программированием и информационными технологиями, основанными на достижениях науки информатики и научно-технического прогресса;

осознанный выбор и построение индивидуальной траектории образования и жизненных планов с учётом личных и общественных интересов и потребностей;

7) экологического воспитания:

осознание глобального характера экологических проблем и путей их решения, в том числе с учётом возможностей информационных и коммуникационных технологий;

8) адаптации обучающегося к изменяющимся условиям социальной и природной среды:

освоение обучающимися социального опыта, основных социальных ролей, соответствующих ведущей деятельности возраста, норм и правил общественного поведения, форм социальной жизни в группах и сообществах, в том числе существующих в виртуальном пространстве.

МЕТАПРЕДМЕТНЫЕ РЕЗУЛЬТАТЫ

Метапредметные результаты освоения программы по информатике отражают овладение универсальными учебными действиями –

познавательными, коммуникативными, регулятивными.

Познавательные универсальные учебные действия

Базовые логические действия:

умение определять понятия, создавать обобщения, устанавливать аналогии, классифицировать, самостоятельно выбирать основания и критерии для классификации, устанавливать причинно-следственные связи, строить логические рассуждения, делать умозаключения (индуктивные, дедуктивные и по аналогии) и выводы;

умение создавать, применять и преобразовывать знаки и символы, модели и схемы для решения учебных и познавательных задач;

самостоятельно выбирать способ решения учебной задачи (сравнивать несколько вариантов решения, выбирать наиболее подходящий с учётом самостоятельно выделенных критериев).

Базовые исследовательские действия:

формулировать вопросы, фиксирующие разрыв между реальным и желательным состоянием ситуации, объекта, и самостоятельно устанавливать искомое и данное;

оценивать на применимость и достоверность информацию, полученную в ходе исследования;

прогнозировать возможное дальнейшее развитие процессов, событий и их последствия в аналогичных или сходных ситуациях, а также выдвигать предположения об их развитии в новых условиях и контекстах.

Работа с информацией:

выявлять дефицит информации, данных, необходимых для решения поставленной задачи;

применять различные методы, инструменты и запросы при поиске и отборе информации или данных из источников с учётом предложенной учебной задачи и заданных критериев;

выбирать, анализировать, систематизировать и интерпретировать информацию различных видов и форм представления;

самостоятельно выбирать оптимальную форму представления информации и иллюстрировать решаемые задачи несложными схемами, диаграммами, иной графикой и их комбинациями;

оценивать надёжность информации по критериям, предложенным учителем или сформулированным самостоятельно;

эффективно запоминать и систематизировать информацию.

Коммуникативные универсальные учебные действия

Общение:

сопоставлять свои суждения с суждениями других участников диалога,

обнаруживать различие и сходство позиций;

публично представлять результаты выполненного опыта (эксперимента, исследования, проекта);

самостоятельно выбирать формат выступления с учётом задач презентации и особенностей аудитории и в соответствии с ним составлять устные и письменные тексты с использованием иллюстративных материалов.

Совместная деятельность (сотрудничество):

понимать и использовать преимущества командной и индивидуальной работы при решении конкретной проблемы, в том числе при создании информационного продукта;

принимать цель совместной информационной деятельности по сбору, обработке, передаче, формализации информации, коллективно строить действия по её достижению: распределять роли, договариваться, обсуждать процесс и результат совместной работы;

выполнять свою часть работы с информацией или информационным продуктом, достигая качественного результата по своему направлению и координируя свои действия с другими членами команды;

оценивать качество своего вклада в общий информационный продукт по критериям, самостоятельно сформулированным участниками взаимодействия;

сравнивать результаты с исходной задачей и вклад каждого члена команды в достижение результатов, разделять сферу ответственности и проявлять готовность к предоставлению отчёта перед группой.

Регулятивные универсальные учебные действия

Самоорганизация:

выявлять в жизненных и учебных ситуациях проблемы, требующие решения;

ориентироваться в различных подходах к принятию решений (индивидуальное принятие решений, принятие решений в группе);

самостоятельно составлять алгоритм решения задачи (или его часть), выбирать способ решения учебной задачи с учётом имеющихся ресурсов и собственных возможностей, аргументировать предлагаемые варианты решений;

составлять план действий (план реализации намеченного алгоритма решения), корректировать предложенный алгоритм с учётом получения новых знаний об изучаемом объекте;

делать выбор в условиях противоречивой информации и брать ответственность за решение.

Самоконтроль (рефлексия):

владеть способами самоконтроля, самомотивации и рефлексии;

давать оценку ситуации и предлагать план её изменения;

учитывать контекст и предвидеть трудности, которые могут возникнуть при решении учебной задачи, адаптировать решение к меняющимся обстоятельствам;

объяснять причины достижения (недостижения) результатов информационной деятельности, давать оценку приобретённому опыту, уметь находить позитивное в произошедшей ситуации;

вносить коррективы в деятельность на основе новых обстоятельств, изменившихся ситуаций, установленных ошибок, возникших трудностей;

оценивать соответствие результата цели и условиям.

Эмоциональный интеллект:

ставить себя на место другого человека, понимать мотивы и намерения другого.

Принятие себя и других:

осознавать невозможность контролировать всё вокруг даже в условиях открытого доступа к любым объёмам информации.

ПРЕДМЕТНЫЕ РЕЗУЛЬТАТЫ

К концу обучения в **5 классе** у обучающегося будут сформированы следующие умения:

ответственно выбирать оптимальные и безопасные пути освоения цифровых технологий, Интернета и цифровых устройств;

находить оптимальные способы решения проблем, возникающих в процессе освоения Интернета и цифровых технологий;

ответственно и безопасно использовать различные способы подключения к Интернету и возможности их настройки в соответствии с текущими задачами, а также осваивать новые средства связи;

ответственно и безопасно использовать различные поисковые системы и их возможности для поиска в Интернете информации, необходимой для решения различных жизненных задач, в том числе образовательных;

ответственно и безопасно взаимодействовать с другими пользователями на различных интернет-ресурсах (в социальных сетях) в соответствии с общечеловеческими нормами поведения, текущим законодательством РФ, правилами конкретного интернет-ресурса, а также в зависимости от оценки сложившейся ситуации;

оценивать качество продуктов, предоставляемых на различных интернет-ресурсах, а также потенциальные риски, связанные с их потреблением;

различать виды персональных данных и понимать последствия небрежного обращения с ними, способы их попадания в Интернет и дальнейшего распространения в Сети;

разбираться в изменениях, которые происходят в технологической и социальной сферах;

понимать, адекватно и ответственно использовать возможности, которые появляются благодаря новым технологиям.

К концу обучения **в 6 классе** у обучающегося будут сформированы следующие умения:

понимать и адекватно использовать возможности, предоставляемые Интернетом и цифровыми технологиями, в соответствии с этическими нормами и текущим законодательством РФ;

оценивать количество личного времени, проводимого за использованием Интернета и цифровых устройств, и качество содержательного наполнения этого времени;

ответственно и безопасно использовать современное программное обеспечение для работы в Интернете и возможности их настройки в соответствии с текущими задачами, а также осваивать новое программное обеспечение;

оценивать качество информации и информационных ресурсов в Интернете, в том числе их достоверность, надёжность, безопасность, а также потенциальные риски, связанные с их использованием и распространением;

ответственно и безопасно выбирать стратегии коммуникации, в том числе самопрезентации, на различных интернет-ресурсах (в социальных сетях) в зависимости от вида ресурса, целей коммуникации и целевой аудитории;

использовать различные интернет-ресурсы для поиска информации о необходимых товарах и услугах;

уметь пользоваться различными средствами управления персональными данными и приватностью в Интернете;

понимать и адекватно оценивать риски, возникающие вследствие изменений в технологической и социальной сферах.

К концу обучения **в 7 классе** у обучающегося будут сформированы следующие умения:

понимать и адекватно оценивать риски, возникающие в процессе освоения Интернета и цифровых технологий;

ответственно и сбалансированно распределять личное время, в том числе отводимое на использование цифровых технологий;

ответственно и безопасно относиться к конфиденциальности личных данных в Интернете и уметь защищать их от несанкционированного доступа;

ответственно и безопасно использовать программные средства для защиты технических устройств от вирусов;

ответственно и безопасно использовать различные интернет-ресурсы для создания и размещения в Интернете оригинальной позитивной информации (мультимедиа, текстов, сайтов и т.д.);

ответственно и безопасно управлять собственной репутацией (формировать, поддерживать, защищать) и социальным капиталом в Интернете;

ответственно и безопасно использовать интернет-ресурсы, соблюдая пользовательские соглашения и общие правила безопасности;

ответственно и безопасно использовать специальные безопасные режимы работы в браузерах;

ответственно и безопасно использовать приёмы, позволяющие контролировать распространение персональных данных в Интернете, а также удалять следы онлайн-активности с различных устройств и онлайн-ресурсов;

находить личные жизненные ориентиры, соответствующие нравственным и этическим нормам.

К концу обучения в 8 классе у обучающегося будут сформированы следующие умения:

оценивать наличие признаков чрезмерного использования Интернета и цифровых устройств;

находить адекватные, оптимальные пути решения проблемы чрезмерного использования Интернета и цифровых устройств.

оценивать основные риски, связанные с различными способами подключения к Сети, использованием локальных и облачных приложений для работы в Интернете, аутентификацией в Интернете, использованием антивирусных средств для защиты технических устройств.

ответственно и безопасно потреблять и распространять информацию в соответствии с этическими нормами, текущим законодательством РФ в области авторского права и защиты детей от информации, причиняющей вред их здоровью и развитию;

оценивать основные риски использования информации в Интернете, связанные с поиском и оценкой достоверности и надёжности информации, созданием и размещением информационного контента, распространением в Сети противозаконной информации, угрожающей здоровью и развитию детей и подростков.

адекватно оценивать риски, возникающие в процессе коммуникации в Интернете (в случае встречи с незнакомцами, проявления агрессии и т.д.), а также выбирать безопасные стратегии поведения в ситуациях, связанных с этими рисками;

оценивать основные потребительские риски, связанные с приобретением и потреблением товаров и услуг, представленных на различных интернет-ресурсах, распространением рекламы в Интернете, различными

видами мошенничества в Интернете (в том числе фишингом), различными видами онлайн-игр (многопользовательских, социальных, казуальных).

ответственно и безопасно использовать настройки приватности в социальных сетях и на других онлайн-ресурсах;

оценивать основные риски, связанные с предоставлением и распространением персональных данных.

выбирать и планировать адекватный и оптимальный путь реализации личностного потенциала и жизненного плана в условиях цифрового общества и с учётом происходящих изменений.

создавать и планировать жизненный план в условиях цифрового общества и с учётом происходящих изменений.

**ТЕМАТИЧЕСКОЕ ПЛАНИРОВАНИЕ
5 КЛАСС**

№ п/п	Наименование разделов и тем программы	Количество часов		
		Всего	Контрольные работы	Практические работы
Раздел 1. Цифровой мир и интернет-зависимость (3 часа)				
1	Зачем нам нужен Интернет	3		
Раздел 2. Техносфера и технические риски (4 часа)				
2	Как устроен Интернет	4		
Раздел 3. Информация и контентные риски (8 часов)				
3	Какая бывает информация	4		
4	Как работает поиск в Интернете	4		
Раздел 4. Общение и коммуникационные риски (4 часа)				
5	Как люди общаются в Интернете	4		
Раздел 5. Цифровая экономика и потребительские риски (4 часа)				
6	Как совершать покупки в Интернете	4		
Раздел 6. Персональные данные (7 часов)				
7	Что такое персональные данные	4		
8	Какие следы мы оставляем в Интернете	3		
Раздел 7. Цифровое будущее (2 часа)				
9	Урок в школе будущего	2		
	Резервное время	2		
	ОБЩЕЕ КОЛИЧЕСТВО ЧАСОВ ПО ПРОГРАММЕ	34		

6 КЛАСС

№ п/п	Наименование разделов и тем программы	Количество часов		
		Всего	Контрольные работы	Практические работы
Раздел 1. Цифровой мир и интернет-зависимость (3 часа)				
1	Мы в цифровом мире	3		
Раздел 2. Техносфера и технические риски (4 часа)				
2	Почему важны пароли в Интернете	4		
Раздел 3. Информация и контентные риски (8 часов)				
3	Полезные интернет-ресурсы	4		
4	Как искать и распознавать правдивую	4		
Раздел 4. Общение и коммуникационные риски (6 часов)				
5	Как общаться в Интернете	3		
6	Как избежать конфликтов в Интернете	3		
Раздел 5. Цифровая экономика и потребительские риски (4 часа)				
7	Как не попасться на удочку онлайн-	4		
Раздел 6. Персональные данные (5 часов)				
8	Что такое персональные данные	2		
9	Что нужно знать о цифровых следах	3		
Раздел 7. Цифровое будущее (2 часа)				
10	Дома будущего	2		
	Резервное время	2		
	ОБЩЕЕ КОЛИЧЕСТВО ЧАСОВ ПО ПРОГРАММЕ	34		

7 КЛАСС

№ п/п	Наименование разделов и тем программы	Количество часов		
		Всего	Контрольные работы	Практические работы
Раздел 1. Цифровой мир и интернет-зависимость (3 часа)				
1	Как не заблудиться в Интернете	3		
Раздел 2. Техносфера и технические риски (3 часа)				
2	Как безопасно подключаться к Интернету	3		
Раздел 3. Информация и контентные риски (8 часов)				
3	Как искать полезную информацию в Интернете	4		
4	Почему нужно проверять информацию в	4		
Раздел 4. Общение и коммуникационные риски (8 часов)				
5	Человек в Интернете: реальный или виртуальный?	4		
6	Как противостоять агрессии в Интернете	4		
Раздел 5. Цифровая экономика и потребительские риски (3 часа)				
7	Как безопасно совершать покупки в Интернете	3		
Раздел 6. Персональные данные (5 часов)				
8	Как персональные данные оказываются в Сети	3		
9	Для чего нужно управлять персональными данными	2		

Раздел 7. Цифровое будущее (2 часа)				
10	Цифровой мир будущего	2		
	Резервное время	2		
	ОБЩЕЕ КОЛИЧЕСТВО ЧАСОВ ПО ПРОГРАММЕ	34		

8 КЛАСС

№ п/п	Наименование разделов и тем программы	Количество часов		
		Всего	Контрольные работы	Практические работы
Раздел 1. Цифровой мир и интернет-зависимость (3 часа)				
1	Другая реальность — дополненная и виртуальная	3		
Раздел 2. Техносфера и технические риски (4 часа)				
2	Защита от вредоносных программ	4		
Раздел 3. Информация и контентные риски (6 часов)				
3	Как стать мастером поиска в Интернете	3		
4	Фейки в Интернете: как их распознать	3		
Раздел 4. Общение и коммуникационные риски (8 часов)				
5	Репутация в Интернете: как её сохранить	4		
6	Агрессия в Сети: способы предотвращения	4		
Раздел 5. Цифровая экономика и потребительские риски (4 часа)				
7	Электронные платежи: правила безопасности	4		
Раздел 6. Персональные данные (5 часов)				
8	Персональные данные в Сети: как их защитить	3		
9	Оберегаем личное пространство в Интернете	2		

Раздел 7. Цифровое будущее (2 часа)				
10	Профессии будущего	2		
	Резервное время	2		
	ОБЩЕЕ КОЛИЧЕСТВО ЧАСОВ ПО ПРОГРАММЕ	34		

**ПОУРОЧНОЕ ПЛАНИРОВАНИЕ
5 КЛАСС**

№ п/п	Наименование разделов и тем программы	Количество часов			Дата изучения
		Всего	Контрольные работы	Практические работы	
1.	Зачем нам нужен Интернет	1			
2.	Зачем нам нужен Интернет	1			
3.	Зачем нам нужен Интернет	1			
4.	Как устроен Интернет	1			
5.	Как устроен Интернет	1			
6.	Как устроен Интернет	1			
7.	Как устроен Интернет	1			
8.	Какая бывает информация	1			
9.	Какая бывает информация	1			
10.	Какая бывает информация	1			
11.	Какая бывает информация	1			
12.	Как работает поиск в Интернете	1			
13.	Как работает поиск в Интернете	1			
14.	Как работает поиск в Интернете	1			
15.	Как работает поиск в Интернете	1			
16.	Как люди общаются в Интернете	1			
17.		1			

18.	Как люди общаются в Интернете	1			
19.	Как люди общаются в Интернете	1			
20.	Как совершать покупки в Интернете	1			
21.	Как совершать покупки в Интернете	1			
22.	Как совершать покупки в Интернете	1			
23.	Как совершать покупки в Интернете	1			
24.	Что такое персональные данные	1			
25.	Что такое персональные данные	1			
26.	Что такое персональные данные	1			
27.	Что такое персональные данные	1			
28.	Какие следы мы оставляем в Интернете	1			
29.	Какие следы мы оставляем в Интернете	1			
30.	Какие следы мы оставляем в Интернете	1			
31.	Урок в школе будущего	1			
32.	Урок в школе будущего	1			
	Резервное время	2			
	ОБЩЕЕ КОЛИЧЕСТВО ЧАСОВ ПО ПРОГРАММЕ	34			

6 КЛАСС

№ п/п	Наименование разделов и тем программы	Количество часов			Дата изучения
		Всего	Контрольные работы	Практические работы	
1.	Мы в цифровом мире	1			
2.	Мы в цифровом мире	1			
3.	Мы в цифровом мире	1			
4.	Почему важны пароли в Интернете	1			
5.	Почему важны пароли в Интернете	1			
6.	Почему важны пароли в Интернете	1			
7.	Почему важны пароли в Интернете	1			
8.	Полезные интернет-ресурсы	1			
9.	Полезные интернет-ресурсы	1			
10.	Полезные интернет-ресурсы	1			
11.	Полезные интернет-ресурсы	1			
12.	Как искать и распознавать правдивую	1			
13.	Как искать и распознавать правдивую	1			
14.	Как искать и распознавать правдивую	1			
15.	Как искать и распознавать правдивую	1			
16.	Как общаться в Интернете	1			
17.	Как общаться в Интернете	1			
18.	Как общаться в Интернете	1			
19.	Как избежать конфликтов в Интернете	1			

20.	Как избежать конфликтов в Интернете	1			
21.	Как избежать конфликтов в Интернете	1			
22.	Как не попасться на удочку онлайн-	1			
23.	Как не попасться на удочку онлайн-	1			
24.	Как не попасться на удочку онлайн-	1			
25.	Как не попасться на удочку онлайн-	1			
26.	Что такое персональные данные	1			
27.	Что такое персональные данные	1			
28.	Что нужно знать о цифровых следах	1			
29.	Что нужно знать о цифровых следах	1			
30.	Что нужно знать о цифровых следах	1			
31.	Дома будущего	1			
32.	Дома будущего	1			
	Резервное время	2			
	ОБЩЕЕ КОЛИЧЕСТВО ЧАСОВ ПО ПРОГРАММЕ	34			

7 КЛАСС

№ п/п	Наименование разделов и тем программы	Количество часов			Дата изучения
		Всего	Контрольные работы	Практические работы	
1.	Как не заблудиться в Интернете	1			
2.	Как не заблудиться в Интернете	1			
3.	Как не заблудиться в Интернете	1			
4.	Как безопасно подключаться к Интернету	1			
5.	Как безопасно подключаться к Интернету	1			
6.	Как безопасно подключаться к Интернету	1			
7.	Как искать полезную информацию в Интернете	1			
8.	Как искать полезную информацию в Интернете	1			
9.	Как искать полезную информацию в Интернете	1			
10.	Как искать полезную информацию в Интернете	1			
11.	Почему нужно проверять информацию в	1			
12.	Почему нужно проверять информацию в	1			
13.	Почему нужно проверять информацию в	1			
14.	Почему нужно проверять информацию в	1			
15.	Человек в Интернете: реальный или виртуальный?	1			

16.	Человек в Интернете: реальный или виртуальный?	1			
17.	Человек в Интернете: реальный или виртуальный?	1			
18.	Человек в Интернете: реальный или виртуальный?	1			
19.	Как противостоять агрессии в Интернете	1			
20.	Как противостоять агрессии в Интернете	1			
21.	Как противостоять агрессии в Интернете	1			
22.	Как противостоять агрессии в Интернете	1			
23.	Как безопасно совершать покупки в Интернете	1			
24.	Как безопасно совершать покупки в Интернете	1			
25.	Как безопасно совершать покупки в Интернете	1			
26.	Как персональные данные оказываются в Сети	1			
27.	Как персональные данные оказываются в Сети	1			
28.	Как персональные данные оказываются в Сети	1			

29.	Для чего нужно управлять персональными данными	1			
30.	Для чего нужно управлять персональными данными	1			
31.	Цифровой мир будущего	1			
32.	Цифровой мир будущего	1			
	Резервное время	2			
	ОБЩЕЕ КОЛИЧЕСТВО ЧАСОВ ПО ПРОГРАММЕ	34			

8 КЛАСС

№ п/п	Наименование разделов и тем программы	Количество часов			Дата изучения
		Всего	Контрольные работы	Практические работы	
1.	Другая реальность — дополненная и	1			
2.	Другая реальность — дополненная и	1			
3.	Другая реальность — дополненная и	1			
4.	Защита от вредоносных программ	1			
5.	Защита от вредоносных программ	1			
6.	Защита от вредоносных программ	1			
7.	Защита от вредоносных программ	1			
8.	Как стать мастером поиска в Интернете	1			
9.	Как стать мастером поиска в Интернете	1			
10.	Как стать мастером поиска в Интернете	1			
11.	Фейки в Интернете: как их распознать	1			
12.	Фейки в Интернете: как их распознать	1			
13.	Фейки в Интернете: как их распознать	1			
14.	Репутация в Интернете: как её сохранить	1			
15.	Репутация в Интернете: как её сохранить	1			
16.	Репутация в Интернете: как её сохранить	1			
17.	Репутация в Интернете: как её сохранить	1			

18.	Агрессия в Сети: способы предотвращения	1			
19.	Агрессия в Сети: способы предотвращения	1			
20.	Агрессия в Сети: способы предотвращения	1			
21.	Агрессия в Сети: способы предотвращения	1			
22.	Электронные платежи: правила безопасности	1			
23.	Электронные платежи: правила безопасности	1			
24.	Электронные платежи: правила безопасности	1			
25.	Электронные платежи: правила безопасности	1			
26.	Персональные данные в Сети: как их защитить	1			
27.	Персональные данные в Сети: как их защитить	1			
28.	Персональные данные в Сети: как их защитить	1			
29.	Оберегаем личное пространство в Интернете	1			

30.	Оберегаем личное пространство в Интернете	1			
31.	Профессии будущего	1			
32.	Профессии будущего	1			
	Резервное время	2			
	ОБЩЕЕ КОЛИЧЕСТВО ЧАСОВ ПО ПРОГРАММЕ	34			

УЧЕБНО-МЕТОДИЧЕСКОЕ ОБЕСПЕЧЕНИЕ ОБРАЗОВАТЕЛЬНОГО ПРОЦЕССА ОБЯЗАТЕЛЬНЫЕ УЧЕБНЫЕ МАТЕРИАЛЫ ДЛЯ УЧЕНИКА

1. *Солдатова Г., Зотова Е., Лебешева М., Шляпников В.* Интернет: возможности, компетенции, безопасность: методическое пособие для работников системы общего образования. Ч. 1. Лекции. М.: Центр книжной культуры «Гутенберг», 2013. URL: <http://detionline.com/assets/files/research/BookTheorye.pdf> (дата обращения: 17.06.2022).
2. *Солдатова Г., Зотова Е., Лебешева М., Шляпников В.* Интернет: возможности, компетенции, безопасность: методическое пособие для работников системы общего образования. Ч. 2. Практикум. М.: Центр книжной культуры «Гутенберг», 2013. URL: http://detionline.com/assets/files/research/Book_Praktikum.pdf (дата обращения: 17.06.2022).
3. *Солдатова Г.У., Нестик Т.А., Рассказова Е.И., Зотова Е.Ю.* Цифровая компетентность подростков и родителей. Результаты всероссийского исследования. М.: Фонд Развития Интернет, 2013. URL: <http://detionline.com/assets/files/research/DigitalLiteracy.pdf> (дата обращения: 17.06.2022).
4. *Солдатова Г.У., Приезжева А.А., Олькина О.И., Шляпников В.Н.* Практическая психология безопасности. Управление персональными данными в интернете: учебно-методическое пособие для работников системы общего образования. 2-е. изд., испр. и доп. М.: Генезис, 2017. URL: <http://detionline.com/assets/files/research/Internetbezopasnost.pdf> (дата обращения: 17.06.2022).
5. *Солдатова Г., Рассказова Е., Зотова Е., Лебешева М., Роггендорф П.* Дети России онлайн: риски и безопасность. Результаты международного проекта EU Kids Online II в России. URL: http://detionline.com/assets/files/helpline/RussianKidsOnline_Final%20ReportRussian.pdf (дата обращения: 17.06.2022).
6. *Солдатова Г.У., Рассказова Е.И., Нестик Т.А.* Цифровое поколение России: компетентность и безопасность. М.: Смысл, 2017. URL: http://detionline.com/assets/files/research/2017_cifrovoe_pokolenie_rossii.pdf (дата обращения: 17.06.2022).
7. *Солдатова Г.У.* Цифровая социализация в культурно-исторической парадигме: изменяющийся ребёнок в изменяющемся мире // Социальная психология и общество. 2018. Т. 9. № 3. С. 71-80.

8. *Солдатова Г.У., Чигарькова С.В., Дренёва АА., Илюхина С.Н.* Мы в ответе за цифровой мир. Профилактика деструктивного поведения подростков и молодёжи в Интернете: учебно-методическое пособие. М.: Когито-Центр, 2019. URL: http://detionline.com/assets/files/research/my_v_otvete_za_cifrovoy_mir.pdf (дата обращения: 17.06.2022).
9. *Солдатова Г.У., Чигарькова С.В., Илюхина С.Н.* Социокультурные онлайн-практики в молодёжной среде. Мы в ответе за цифровой мир: учебное пособие. М.: Когито-Центр, 2021.

МЕТОДИЧЕСКИЕ МАТЕРИАЛЫ ДЛЯ УЧИТЕЛЯ

1. *Блау М.* Удивительный Интернет. М.: Энас-книга, 2016. С. 432.
2. *Бочавер АА., Хломов К.Д.* Буллинг как объект исследований и культурный феномен // Психология: журнал Высшей школы экономики. 2013. Т. 10. № 3.
3. *Бочавер АА., Хломов К.Д.* Кибербуллинг: травля в пространстве современных технологий // Психология: журнал Высшей школы экономики. 2014. Т. 11. № 3.
4. *Голубева НА., Марцинковская Т.Д.* Информационная социализация: психологический подход // Психологические исследования: электронный научный журнал. 2011. № 6. С. 2.
5. *Голубева НА., Марцинковская Т.Д.* Социализация современных подростков: информационный контекст // Вопросы психологии. 2016. № 5. С. 15-28.
6. *Жичкина А.Е., Белинская Е.П.* Самопрезентация в виртуальной коммуникации и особенности идентичности подростков — пользователей Интернета // Образование и информационная культура. Социологические аспекты. Труды по социологии образования. 2000. С.431-460.
7. Информационные и коммуникационные технологии в образовании: монография / под ред. Б. Дендева. М.: ИИТО ЮНЕСКО, 2013.
8. *Карр Н.* Пустышка. Что Интернет делает с нашими мозгами. СПб.: Бест Бизнес Букс, 2012.
9. *Кин Э.* Ничего личного. М.: Альпина паблишер, 2016.
10. *Манович Л.* Язык новых медиа / Л. Манович; [перевод Дианы Кульчицкой]. М.: Ad Marginem Press, 2018.
11. *Марцинковская Т.Д.* Информационная социализация в изменяющемся информационном пространстве // Психологические исследования: электронный научный журнал. 2012. Т. 5. № 26. С. 7.
12. Медийная и информационная грамотность: программа обучения педагогов. М.: Институт ЮНЕСКО по информационным технологиям в образовании, 2012.

13. *Палфри Дж., Гассер У.* Дети цифровой эры. М.: Эксмо, 2011.
14. *Скиннер К.* Человек цифровой: четвёртая революция в истории человечества, которая затронет каждого / пер. с англ. О. Сивченко; науч. ред. К. Щеглова. М.: Манн, Иванов и Фербер, 2019.
15. *Солдатова Г.У., Вишнева А.Е.* Особенности развития когнитивной сферы у детей с разной онлайн-активностью: есть ли золотая середина? // Консультативная психология и психотерапия. 2019. Т. 27. №3. С. 97-118. URL: https://psyjournals.ru/files/108516/cpp_2019_n3_Soldatova_Vishneva.pdf (дата обращения: 17.06.2022).
16. *Солдатова Г., Зотова Е, Чекалина А., Гостимская О.* Пойманные одной сетью // Социально-психологическое исследование восприятия интернета детьми и подростками. М., 2011.
17. *Солдатова Г.У., Рассказова Е.И.* Неосведомлённость родителей о столкновении подростков с рисками в Интернете: содержание и психологические факторы // Психологический журнал. 2019. Т. 40. № 1. С. 71-83.
18. *Солдатова Г.У., Рассказова Е.И.* «Оборотная сторона» цифровой компетентности российских подростков: иллюзия компетентности и рискованное поведение онлайн // Вопросы психологии. 2017. № 3. С. 3-15.
19. *Солдатова Г.У., Рассказова Е.И.* Цифровая ситуация развития межпоколенческих отношений: разрыв и взаимодействие между подростками и родителями в Интернете // Мир психологии. 2017. № 1 (89). С. 134-143.
20. *Солдатова Г.У., Рассказова Е.И., Чигарькова С.В., Львова Е.Н.* Цифровая культура: правила, ответственность и регуляция // Цифровое общество как культурно-исторический контекст развития человека: сборник научных статей и материалов международной конференции, 14-17 февраля 2018, Коломна / под общ. ред. Р.В. Ершовой. Коломна: Государственный социально-гуманитарный университет, 2018. С. 374-379.
21. *Солдатова Г.У., Шляпников В.Н.* Цифровая компетентность российских педагогов // Психологическая наука и образование. 2015. Т. 20. № 4. С. 5-18.
22. *Солдатова Г.У., Ярмина А.Н.* Кибербуллинг: особенности, ролевая структура, детско-родительские отношения и стратегии совладания // National Psychological Journal. 2019. Т. 12. № 3.
23. *Цымбаленко С.Б.* Подросток в информационном мире: практика социального проектирования. М.: НИИ Школьных технологий, 2010.
24. Digital Competence Framework for Educators (DigCompEdu). Published on EU Science Hub. URL: <https://ec.europa.eu/jrc/en/printpdf/137812> (дата обращения: 17.06.2022).
25. *Mossberger K., Tolbert C.J., McNeal R.S.* Digital Citizenship. The Internet, Society and Participation. Cambridge, Massachusetts: MIT Press, 2007.

26. *Smahel D., et al.* EU Kids Online 2020: survey results from 19 countries. 2020.

ЦИФРОВЫЕ ОБРАЗОВАТЕЛЬНЫЕ РЕСУРСЫ И РЕСУРСЫ СЕТИ

ИНТЕРНЕТ

1. Дети России онлайн — сайт проектов Фонда Развития Интернет [Электронный ресурс]: [сайт]. [2020]. URL: <http://detionline.com> (дата обращения: 18.06.2022).
2. Образовательный портал для родителей от Лаборатории Касперского [Электронный ресурс]: [сайт]. [2017]. URL: <https://kids.kaspersky.ru> (дата обращения: 18.06.2022).
3. Электронные версии выпусков журнала «Дети в информационном обществе» [Электронный ресурс]: [сайт]. [2017]. URL: <http://detionline.com/journal/numbers> (дата обращения: 18.06.2022).