УПРАВЛЕНИЕ ОБРАЗОВАНИЯ
АДМИНИСТРАЦИИ МУНИЦИПАЛЬНОГО
ОБРАЗОВАНИЯ ДИНСКОЙ РАЙОН

МУНИЦИПАЛЬНО БЮДЖЕТНОЕ ОБЩЕОБРАЗОВАТЕЛЬНОЕ
УЧРЕЖДЕНИЕМУНИЦИПАЛЬНОГО ОБРАЗОВАНИЯ ДИНСКОЙ
РАЙОН
«СРЕДНЯЯ ОБЩЕОБРАЗОВАТЕЛЬНАЯ
ШКОЛА №10ИМЕНИ БРАТЬЕВ
ИГНАТОВЫХ»

Принята на заседании педагогическо советаМБОУ СОШ №10
Протокол №___от_____г.

Подписано цифровой подписью: Ефременко Светлана Михайловна
DN: cn=Ефременко Светлана Михайловна, o=МБОУ СОШ №10 им. братьев Игнатовых МО Динской район, ou=директор, email=school10@din.kubannet.ru, c=RU
Дата: 2022.11.13 00:37:13 +03'00'

Утверждаю
Директор МБОУ СОШ №10
_____С.М.
Ефременко Приказ №_____от____г.

ДОПОЛНИТЕЛЬНАЯ ОБЩЕОБРАЗОВАТЕЛЬНАЯ ОБЩЕРАЗВИВАЮЩАЯ ПРОГРАММА

ТЕХНИЧЕСКОЙ НАПРАВЛЕННОСТИ

«Информационная безопасность»

Уровень программы: базовый
Срок реализации программы: 5 лет (170 часов)
Возрастная категория: от 10 до 16 лет
Форма обучения: очная
Программа реализуется на бюджетной основе

Автор-составитель:
Калинина Антонина Сергеевна,
педагог дополнительного образования

ст. Васюринская, 2022

Раздел I«Основные характеристики программы»

1.1 Пояснительная записка

Настоящая программа «Информационная безопасность» разработана на основе авторской программы курса «Кибербезопасность» (Программа курса «Кибербезопасность». 5–9 классы / Г.У. Солдатова, С.В. Чигарькова, И.Д. Пермякова. — М.: ООО «Русское слово — учебник», 2022. — 32 с. — (ФГОС)). Внесены изменения в структурно-содержательный аспект и условия организации образовательного процесса.

Социальная среда, в которой растут современные дети, сильно отличается от той, что формировала их родителей. Цифровые технологии проникают во все сферы жизни. На наших глазах формируется цифровое общество, и одним из важных факторов социализации в нём становится Интернет.

Компьютер, подключённый к Сети, — влиятельный по средник между взрослым миром и детьми. Сегодня в значительной степени благодаря ему расширяется зона ближайшего развития ребёнка — область не созревших, а только созревающих психических функций, его образовательный потенциал. Понятие зоны ближайшего развития было предложено известным отечественным психологом Л. С. Выготским и активно используется как в российской, так и в зарубежной детской психологии. В условиях цифрового общества зона ближайшего развития определяется не только непосредственным взаимодействием ребёнка со взрослым, но и многочисленными взаимодействиями с миром, представленным в Интернете.

Современные подростки выстраивают каналы информации для общения с ровесниками и взрослыми, где сами же являются участниками равноправногодиалога, проявляют активность, влияющую на социальное окружение**.** Иными словами, они создают коммуникативные сообщества, в которых информационная составляющая становится важной частью группового общения.

Направленность программы – техническая. Образовательная программа «Медиастудия» предназначена для работы с учащимися БОУ СОШ № 10 МО Динской район и нацелена на формирование творческой индивидуальности, приобретение ребенком основ работы в медиаиндустрии и создание медиа продуктов на актуальные темы.

Актуальность программы.

Отличительной особенностью социализации в Интернете является её стихийный, неконтролируемый характер. Зачастую современные дети осваивают цифровые технологии самостоятельно, без присмотра со стороны взрослого. Родители чувствуют себя гораздо спокойнее, когда их ребёнок сидит за компьютером в соседней комнате, нежели когда он «пропадает неизвестно где»; они полагают, что таким образом он избегает негативного влияния «улицы», недооценивая при этом риски, связанные с цифровой социализацией. Однако Интернет — это та же «улица»

протяжённостью в миллионы гигабайтов, и там ребёнок, предоставленный самому себе, может повстречаться с разными ситуациями.

Попадая в Интернет из самых защищённых и безопасных мест — из дома или школы, — дети и подростки относятся к киберпространству с большим доверием. Способность оценить степень опасности той или иной среды приходит с жизненным опытом, это он учит нас предвосхищать нежелательные последствия тех или иных действий, вовремя оценивать разного рода угрозы. Юный пользователь, захваченный безграничными возможностями современных технологий, подобен очарованному страннику: он не может разглядеть риски, которые встречаются в Сети, и оказывается одним из самых незащищённых и уязвимых её пользователей. Когда он понимает, что столкнулся в Сети с непосредственной опасностью, то часто не знает, как поступить и к кому обратиться за помощью, и вынужден учиться на собственных ошибках. Взрослым важно понимать, что риски онлайн-среды связаны не только с содержанием тех или иных интернет-сайтов, от знакомства с которыми ребёнка следует уберечь. Немалую опасность представляет сам стихийный и неконтролируемый процесс освоения цифрового мира. Как отмечал Л. С. Выготский, обучение должно идти впереди развития. Для того чтобы ребёнок мог безопасно осваиваться в киберпространстве, ему нужен проводник, и стать такими проводниками должны в первую очередь родители и учителя. Только в совместной деятельности со взрослыми процесс цифровой социализации детей может приобрести систематический целенаправленный характер. В соответствии с Федеральными государственными образовательными стандартами обучение в школе осуществляется с использованием современных технологий. На школе лежит ответственность за развитие у детей цифровой компетентности и обучение их навыкам безопасной работы в киберпространстве. Эти направления работы — необходимое условие развития в школе информационной образовательной среды. Стимулируя детей к освоению разных видов деятельности в Сети и одновременно обучая их критически оценивать интернет-ресурсы, развивая навыки безопасного поведения в киберпространстве, мы увеличиваем преимущества, которые даёт обучение с использованием Интернета.

В широком смысле задача взрослых состоит в воспитании «цифрового гражданина», который, с одной стороны, обладает определёнными техническими навыками и компетенциями, с помощью которых он может осуществлять поиск и работу с информацией, налаживать эффективную коммуникацию с другими пользователями Сети, а с другой — использует цифровые технологии безопасно, ответственно и критично. Таким образом, высокая востребованность методических пособий и обучающих программ по формированию и повышению цифровой компетентности определяется следующими факторами:

• Интернет — неотъемлемая часть жизни нового поколения и важный фактор социализации современных детей и подростков;

• дети и подростки активно используют Интернет в образовательных целях, и значительная часть родителей осознаёт образовательный потенциал Интернета;

• требования современной, технологически оснащённой среды мотивируют детей и подростков к повышению своей цифровой компетентности;

• уровень цифровой компетентности современных подростков не может обеспечить эффективное, ответственное и безопасное использование Интернета;

• абсолютное большинство детей и подростков учатся использовать Интернет самостоятельно и бессистемно;

• современная школа естественным образом становится местом, где происходит цифровая социализация детей и подростков, овладение навыками безопасного использования Интернета.

Новизна и особенность программы состоит в том, что в результате образовательной деятельности обучающийся создает безопасное информационное пространство, обеспечивающее решение учебно-воспитательных задач, а также способствующее формированию интегративного взаимодействия в социокультурном пространстве.

Педагогическая целесообразность Программа строится на изучении такого многогранного явления, как Интернет, акцент ставится на изучение правил безопасности онлайн-среды. Занимаясь в объединении, дети узнают, как распознать угрозы в сети, как организовать свое информационное пространство. Абсолютное большинство детей и подростков учатся использовать Интернет самостоятельно и бессистемно, занятия по программе естественным образом помогают добиться цифровой социализации детей и подростков, овладения ими навыком безопасного использования Интернета, а также повышают цифровую компетенцию обучающихся.

Отличительными особенностями программы является ее направленность на повышение цифровой грамотности обучающихся: на занятиях программы «Информационная безопасность» обучающиеся знакомятся с разными возможностями Интернета, учатся вовремя распознавать онлайн-риски (технические, контентные, коммуникационные, потребительские и риск интернет-зависимости), успешно разрешать проблемные ситуации в Сети, защищать свои персональные данные и управлять ими.

Адресат программы.

Программа рассчитана на детей в возрасте от 10 до 16 лет (средний возраст).

Средний школьный возраст: жизнь подростка характеризуется глубокой перестройкой всего организма, общим подъѐмом жизнедеятельности, а также неровностей поведения, непомерным азартом. Это период перехода от детства к юности. В подростковом возрасте резко повышает потребность в активном познании. Еще большие возможности для ускоренного развития деловых качеств детей – подростков открывает трудовая деятельность, когда дети участвуют в ней на равных правах с взрослыми. Важно, чтобы в этом возрасте детям предоставлялся максимум самостоятельности, чтобы взрослыми замечались и поддерживались любые проявления детской инициативы, деловитости, предприимчивости, практической сметки.

Программа позволяет приобрести цифровые компетенции в области формирования безопасного интернет-пространства. Она рассчитана на170 часов.

Формирование групп ведется согласно нормам СанПиН и Уставу МАОУ СОШ № 10 им. братьев Игнатовых. Наполняемость группы 10 – 15 человек. При наборе в группы нет никаких ограничений кроме возраста - принимаются дети от 10 до 16 лет с любым уровнем знаний в сфере кибербезопасности.

Уровень программы, объем и срок реализации программы. Программа реализуется на базовом уровне, рассчитана на 5 лет обучения - 170 часов (1 час в неделю/34 часа в год).

Форма обучения: очная. Форма организации деятельности – групповая.

Режим занятий, периодичность и продолжительность занятий. Занятия проводятся с группой учащихся численностью от 10 до 15 человек 1 раз в неделю по 1 часу. Продолжительность занятий 40 минут, перерыв между занятиями 15 минут.

Особенности организации образовательного процесса.

Обучение по **п**рограмме «Информационная безопасность» организовано в соответствии с системно-деятельностным подходом к обучению, предполагает применение активных методов, совместную работу обучающихся и преподавателя, поиск информации в разных источниках, творческий подход к решению учебных задач. Занятия включают аудиторную и самостоятельную работу. В рамках каждого тематического модуля предполагается вступительная лекционная часть, подготовленная учителем на основе информации, которую он найдёт в методических пособиях, а также в дополнительной литературе и интернет-источниках (см. список литературы и интернет-источников). Задания, представленные в учебниках, рассчитаны на разные формы работы — индивидуальную, в парах, в малых и больших группах. Задания могут выполняться в тетради, с использованием цифровых устройств и в интерактивной форме. По усмотрению учителя некоторые задания могут быть выполнены в формате конференций, круглых столов, выставок, конкурсов. Каждое задание обозначено иконкой, соответствующей его формату. Для создания позитивной атмосферы и повышения мотивации обучающихся введён сквозной персонаж — «персональный помощник» (1-2 год обучения это Кибернешка, в 2-3 год обучения — магистр Кибер Нетов, в 5 год обучения — профессор Кибер Нетович). Текст учебников оформлен как «посты» персонального помощника в социальной сети. В начале каждого учебника персональный помощник даёт информационно-мотивационную справку об Интернете и знакомит читателей с основными рубриками своих «постов». Названия рубрик оформлены как хештеги в социальной сети. В задания также введены сквозные персонажи — школьники Гоша Геймеров, Рита Картинкина и Игорь Неюзеров. Характеры этих персонажей соответствуют разным типам пользователей. Гоша Геймеров — любитель игр, для него Интернет в первую очередь место для онлайн-игр. Рита Картинкина — общительный пользователь, для неё Интернет — место для общения и самопрезентации. Игорь Неюзеров —

любознательный пользователь, для него Интернет прежде всего служит источником информации.

Содержание курса разделено на семь модулей:

1. Цифровой мир и интернет-зависимость.
2. Техносфера и технические риски.
3. Информация и контентные риски.
4. Общение и коммуникационные риски.
5. Цифровая экономика и потребительские риски.
6. Персональные данные.
7. Цифровое будущее.

Модули 1–6 отражают основные области возможностей и рисков в онлайн-пространстве. Модуль 7 ориентирован на создание позитивного образа цифрового будущего. Такая структура даёт объёмное представление как о преимуществах цифровых технологий, так и о возможных опасностях, которые связаны с активным внедрением технологий в повседневную жизнь. На каждый год обучения представлены все семь модулей. Задания курса направленны на решение двух важнейших задач: мотивировать детей на освоение возможностей Интернета и способствовать освоению эффективных стратегий совладания с рисками в различных онлайн-сферах. Вариативность заданий способствует переключению на разные виды деятельности, в том числе с целью здоровьесбережения, профилактики переутомления и повышения интереса со стороны обучающихся.

Помимо лекционной части, в которой преподаватель даёт детям вводную информацию по каждому модулю, занятия включают индивидуальную и групповую работу, работу в парах, общие обсуждения и дискуссии. По усмотрению преподавателя работа над рядом заданий может быть организована в формате конференций, круглых столов, дебатов, выставок, конкурсов.

1.2. Цели и задачи программы

Цели программы «Информационная безопасность» — формирование цифровой компетентности обучающихся и расширение возможностей полезного, критичного, ответственного и безопасного использования Интернета.

Данная программа предполагает решение следующих задач:

• расширить у обучающихся диапазон возможностей, связанных с использованием цифровых технологий;

• способствовать осознанию учащимися влияния, которое цифровые технологии оказывают на их образ жизни;

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

• познакомить обучающихся с возможными онлайн-рисками (техническими, контентными, коммуникационными, потребительскими и риском интернет-зависимости);

• способствовать формированию 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;

• способствовать формированию у обучающихся адекватного образа цифровых технологий, предполагающего, с одной стороны, понимание их позитивной роли в развитии человеческой цивилизации, а с другой — критическую оценку влияния цифровых технологий на разные стороны жизнедеятельности человека;

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

Программа разработана в соответствии с Письмом Минобрнауки РФ от 11.12.2006 г. № 06-1844 «О примерных требованиях к программам дополнительного образования детей», Федеральным законом Российской Федерации «Об образовании в Российской Федерации» от 29 декабря 2012 г. № 273-ФЗ, Порядком организации и осуществления образовательной деятельности по дополнительным общеобразовательным программам (приказ Минобрнауки от 29.08.2013г. № 1008) и отвечает требованиям «Концепции развития дополнительного образования» от 4 сентября 2014 года (Распоряжение Правительства РФ от 04.09.2014 N 1726-р).

1.3. Содержание программы

Учебный план

№	Название модуля, темы	Количество часов			Вид контроля
		Всего	Теория	Практика	
1 год обучения					
	Модуль 1. Цифровой мир и интернет-зависимость (3 часа)				
1	Зачем нам нужен Интернет	3	2	1	Наблюдение
	Модуль 2. Техносфера и технические риски (4 часа				
2	Как устроен Интернет	4	2	2	Опрос
	Модуль 3. Информация и контентные риски (8 часов)				
3	Какая бывает информация	4	2	2	Опрос
4	Как работает поиск в Интернете	4	2	2	Наблюдение
	Модуль 4. Общение и коммуникационные риски (4 часа				
5	Как люди общаются в Интернете	4	2	2	Наблюдение
	Модуль 5. Цифровая экономика и потребительские риски (4 часа)				
6	Как совершать покупки в Интернете	4	2	2	Наблюдение
	Модуль 6. Персональные данные (8 часов)				
7	Что такое персональные данные	4	2	2	Опрос
8	Какие следы мы оставляем в Интернете	4	2	2	Наблюдение
	Модуль 7. Цифровое будущее (3 часа				
9	Урок в школе будущего	3	1	2	Проект
	Итого за год	**34**	**17**	**17**	
2 год обучения					
	Модуль 1. Цифровой мир и интернет-зависимость (3 часа)				
1	Мы в цифровом мире	3	1	2	Наблюдение
	Модуль 2. Техносфера и технические риски (4 часа				
2	Почему важны пароли в Интернете	4	2	2	Опрос
	Модуль 3. Информация и контентные риски (8 часов)				
3	Полезные интернет-ресурсы	4	2	2	Наблюдение
4	Как искать и распознавать правдивую информацию	4	2	2	Опрос
	Модуль 4. Общение и коммуникационные риски (6 часов)				
5	Как общаться в Интернете	3	2	1	Опрос
6	Как избежать конфликтов в Интернете	3	2	1	Наблюдение
	Модуль 5. Цифровая экономика и потребительские риски (4 часа)				
7	Как не попасться на удочку онлайн-мошенникам	4	2	2	Наблюдение
	Модуль 6. Персональные данные (6 часов)				
8	Что такое персональные данные	2	1	1	Опрос
9	Что нужно знать о цифровых следах	4	2	2	Наблюдение
	Модуль 7. Цифровое будущее (3 часа)				
10	Дома будущего	3	1	2	Проект
	Итого за год	34	17	17	
3 год обучения					
	Модуль 1. Цифровой мир и интернет-зависимость (3 часа)				

1	Как не заблудиться в Интернет	3	1	2	
	Модуль 2. Техносфера и технические риски (3 часа)				
2	Как безопасно подключаться к Интернету	3	2	1	Наблюдение
	Модуль 3. Информация и контентные риски (8 часов)				
3	Как искать полезную информацию в Интернете	4	2	2	Опрос
4	Почему нужно проверять информацию в Интернете	4	2	2	Наблюдение
	Модуль 4. Общение и коммуникационные риски (8 часов				
5	Человек в Интернете: реальный или виртуальный?	4	2	2	Наблюдение
6	Как противостоять агрессии в Интернете	4	2	2	Опрос
	Модуль 5. Цифровая экономика и потребительские риски (3 часа)				
7	Как безопасно совершать покупки в Интернете	3	1	2	Наблюдение
	Модуль 6. Персональные данные (6 часов)				
8	Как персональные данные оказываются в Сети	3	1	2	Опрос
9	Для чего нужно управлять персональными данными	3	1	2	Наблюдение
	Модуль 7. Цифровое будущее (3 часа)				
10	Цифровой мир будущего	3	1	2	Проект
	Итого за год	34	15	19	
4 год обучения					
	Модуль 1. Цифровой мир и интернет-зависимость (3 часа)				
1	Другая реальность — дополненная и виртуальная	3	1	2	Наблюдение
	Модуль 2. Техносфера и технические риски (4 часа)				
2	Защита от вредоносных програм	4	2	2	
	Модуль 3. Информация и контентные риски (6 часов)				
3	Как стать мастером поиска в Интернет	3	1	2	Наблюдение
4	Фейки в Интернете: как их распознать	3	1	2	Опрос
	Модуль 4. Общение и коммуникационные риски (8 часов)				
5	Репутация в Интернете: как её сохранить	4	2	2	Опрос
6	Агрессия в Сети: способы предотвращения	4	2	2	Наблюдение
	Модуль 5. Цифровая экономика и потребительские риски (4 часа)				
7	Электронные платежи: правила безопасности	4	2	2	Наблюдение
	Модуль 6. Персональные данные (6 часов)				
8	Персональные данные в Сети: как их защитить	3	1	2	Наблюдение
9	Оберегаем личное пространство в	3	1	2	Опрос

	Интернете				
	Модуль 7. Цифровое будущее (3 часа)				
10	Профессии будущего	3	1	2	Проект
	Итого за год	34	14	20	
5 год обучения					
	Модуль 1. Цифровой мир и интернет-зависимость (3 часа)				
1	Искусственный интеллект: что нас ждёт в будущем?	3	1	2	Наблюдение
	Модуль 2. Техносфера и технические риски (3 часа)				
2	Как искать и хранить информацию в Интернете	3	2	1	Опрос
	Модуль 3. Информация и контентные риски (7 часов)				
3	Как увидеть правду в море лжи	3	1	2	Опрос
4	Как соблюдать авторское право в Интернете	4	2	2	Наблюдение
	Модуль 4. Общение и коммуникационные риски (8 часов)				
5	Всегда ли нужно оставаться на связи?	4	2	2	Опрос
6	Комфорт и безопасность в социальных сетях	4	2	2	Наблюдение
	Модуль 5. Цифровая экономика и потребительские риски (4 часа)				
7	Цифровая экономика: не только покупки	4	2	2	Наблюдение
	Модуль 6. Персональные данные (6 часов)				
8	Что знают обо мне цифровые устройства	3	1	2	Опрос
9	Как управлять репутацией и удалять персональные данные в Интернете	3	2	1	Наблюдение
	Модуль 7. Цифровое будущее (3 часа)				
10	«Умный» город	3	1	2	Проект
	Итого за год	34	16	18	
	Итого за весь срок обучения	**170**	**79**	**91**	

Содержание программы

1 год обучения

Тема 1. 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.

Тема 2. 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.

Тема 3. 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.

Тема 4. Как работает поиск в Интернете. Поиск информации. Поисковая система. Полезные ресурсы в Интернете. Контентные риски: столкновение с неприятным онлайн-контентом. Способы защиты от контентных рисков: настройки безопасного поиска и кнопка «пожаловаться на контент».

Тема 5. 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.

Тема 6. 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.

Тема 7. Что такое персональные данные. Общедоступная и персональная информация. Персональные данные. Виды персональных данных.

Тема 8. Какие следы мы оставляем в Интернете. Виды персональных данных, выкладываемых в открытый доступ. Риски размещения персональной информации в открытом доступе. Настройки приватности.

Тема 9. Урок в школе будущего. Современные технологии, используемые в процессе обучения.

2 год обучения

Тема 1. 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.

Тема 2. 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.

Тема 3. 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.

Тема 4. 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.

Тема 5. 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.

Тема 6. 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.

Тема 7. 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.

Тема 8. Что такое персональные данные. Персональные данные. Публичная и персональная информация. Идентификатор личности. Виды персональных данных.

Тема 9. Что нужно знать о цифровых следах. Цифровой след. Понятие приватности. Настройки приватности в цифровых устройствах. Виды кодов (линейный штрихкод и QR-код). Источники приватных сведений о человеке. Рекомендации по управлению приватностью в Интернете.

Тема 10. Дома будущего. Новшества в архитектуре и строительстве, связанные с цифровыми технологиями. Применение цифровых технологий в быту.

3 год обучения

Тема 1. 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.

Тема 2. 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.

Тема 3. 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.

Тема 4. Почему нужно проверять информацию в Интернете. Достоверная и недостоверная информация. Фейковые новости. Признаки недостоверной, фейковой информации.

Тема 5. 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.

Тема 6. 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.

Тема 7. Как безопасно совершать покупки в Интернете. Цифровая экономика. Покупки в Интернете. Риски онлайншопинга. Правила безопасности при совершении покупок онлайн.

Тема 8. 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.

Тема 9. Для чего нужно управлять персональными данными. Значимость персональных данных. Способы управления персональными данными в Интернете. Рекомендации по предотвращению кражи персональных данных.

Тема 10. Цифровой мир будущего. Интернет вещей. Цифровые технологии и предметы повседневного пользования.

4 год обучения

Тема 1. 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.

Тема 2. Защита от вредоносных программ. Вредоносные программы: мифы и реальность. Компьютерный вирус. Виды вредоносных программ. Троянская программа. Способы защиты от технических рисков.

Тема 3. 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.

Тема 4. 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.

Тема 5. 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.

Тема 6. 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.

Тема 7. 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.

Тема 8. Персональные данные в Сети: как их защитить. Государственный контроль над защитой персональных данных, Роскомнадзор. Сайт «Персональныеданные.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.

Тема 9. 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.

Тема 10. Профессии будущего. Цифровые технологии и профессии. Изменения в мире профессий. Новые профессии, связанные с цифровыми технологиями.

5 год обучения

Тема 1. Искусственный интеллект: что нас ждёт в будущем? Искусственный интеллект, машинное обучение, нейросети, глубокое обучение. Применение

искусственного интеллекта в различных сферах жизни. Тест Тьюринга. Чат-боты. Положительные и отрицательные последствия внедрения технологий искусственного интеллекта.

Тема 2. Как безопасно искать и хранить информацию в Интернете. Браузер. Возможности и недостатки разных браузеров. Функции браузеров: сохранение паролей, сохранение истории посещений, запоминание введённых данных, функция защиты от фишинга и вредоносного программного обеспечения, управление всплывающими окнами, управление информацией о местоположении пользователя, управление доступом к камере и микрофону, управление загрузкой файлов. Облачные программы, облачные сервисы, облачные приложения для учёбы. Минусы и плюсы облачных и локальных сервисов.

Тема 3. Как увидеть правду в море лжи. Постправда. Фейковые новости. Советы по определению фейковых новостей. Борьба с распространением фейковых новостей на уровне российского законодательства. Ответственное отношение к репостам. Значимость критического мышления.

Тема 4. Как соблюдать авторское право в Интернете. Авторское право. Виды лицензий авторского права. Копирайт. Проприетарная лицензия. Копилефт. Лицензия Creative Commons. Пиратство, плагиат. Тест на отношение к сетевому пиратству. Статьи Гражданского кодекса Российской Федерации, связанные с вопросами авторского права.

Тема 5. Всегда ли нужно оставаться на связи? Социальные сети, мессенджеры. Общение в мессенджерах и социальных сетях. Чрезмерное увлечение общением в Интернете. Фабинг. FOMO. Прокрастинация. Способы самоконтроля и борьбы с прокрастинацией.

Тема 6. Комфорт и безопасность в социальных сетях. Общение в Интернете и социальных сетях. Риски общения в социальных сетях. Помощь другим пользователям, столкнувшимся с трудностями. Создание комфортной и безопасной атмосферы при общении в Интернете. Нетикет. Службы поддержки в социальных сетях.

Тема 7. Цифровая экономика: не только покупки. Цифровая экономика. Государственная программа «Цифровая экономика Российской Федерации». Цифровая экономика в повседневной жизни. Экономические отношения без посредников. Шеринг-экономика. Меры предосторожности при покупке товаров и услуг без посредников. Краудфандинг, краудсорсинг. Государственные и муниципальные услуги в Интернете.

Тема 8. Что знают обо мне цифровые устройства. Виды персональных данных. Какая информация хранится на смартфонах. Примущества и недостатки хранения информации в смартфонах. «Умные» вещи. «Интернет вещей». Какие персональные данные собирают «умные» вещи. Правила безопасности при установке приложений. Шифрование в мессенджерах.

Тема 9. Как управлять репутацией и удалять персональные данные в Интернете. Цифровые следы. Репутация в Сети. Право на забвение. Рекомендации по удалению персональных данных из Сети. Статья 13.11 Кодекса РФ об административных нарушениях (Нарушение законодательства Российской Федерации в области персональных данных).

Тема 10. «Умный» город «Умные» города. Цифровые технологии в городских инфраструктурах. Беспилотники. Технология Big Data. Фермы-небоскрёбы.

1. 4. Планируемые результаты

Курс позволяет формировать универсальные учебные действия (УУД) в соответствии с требованиями Федерального государственного образовательного стандарта основного общего образования.

К *регулятивным УУД* относятся сформированные у обучающихся в результате освоения данного курса умение ставить цели, задачи, планировать их реализацию и выбирать эффективные пути их достижения; умение выбирать оптимальные способы разрешения проблемных ситуаций, возникающих при использовании Интернета, что особенно важно при осуществлении деятельности, направленной на обеспечение личной безопасности в Интернете.

К *коммуникативным УУД* в контексте данного курса относятся умение учитывать мнение других пользователей при взаимодействии с ними в онлайн-среде; стремление к кооперации, компромиссу, конструктивному взаимодействию; умение устанавливать контакт в онлайн-общении; умение конструктивно разрешать конфликтные ситуации (выявлять, идентифицировать проблемы, искать и оценивать способы разрешения конфликта, принимать решения и реализовывать их); умение планировать взаимодействие (определять цели, способы взаимодействия) с учётом особенностей онлайн-коммуникации.

В рамках курса формируются такие *познавательные УУД*, как умение формулировать познавательную цель при пользовании Интернетом и цифровыми технологиями; умение искать информацию; умение анализировать информацию с целью выделения существенных и несущественных признаков; умение синтезировать информацию; умение критически оценивать достоверность информации; умение выбирать основания и критерии для сравнения информации, устанавливать причинно-следственные связи, выстраивать логические цепи рассуждений, выдвигать гипотезы и обосновывать их.

По итогам освоения курса у обучающихся должен появиться *опыт учебно-исследовательской и проектной деятельности* в онлайн-среде. У обучающихся возникнут познавательные интересы в области цифровых технологий.

Курс позволяет решать ряд *воспитательных задач*. Он обеспечивает наличие у обучающихся знаний основных прав и обязанностей пользователя Интернета в соответствии с законами РФ. Обучающиеся должны научиться ориентироваться в системе моральных норм и ценностей, а также в особенностях взаимоотношений и культуры поведения в онлайн-среде. Обучающиеся осваивают культуру общения в Интернете, учатся способствовать формированию культуры поведения в онлайн-среде среди сверстников. Обучающиеся смогут оценивать поступающую онлайн-информацию, исходя из нравственных и этических норм. Они смогут проводить рефлексию своей деятельности и осознают ответственность за результаты этой деятельности.

В процессе освоения курса у обучающихся формируется доброжелательное отношение к другим пользователям Интернета, нетерпимость к любым формам агрессивного и противоправного поведения в Интернете и готовность противостоять им, а также уважение к общечеловеческим ценностям, готовность к распространению их в онлайн-среде. У обучающихся развивается потребность в личностном росте, самореализации в соответствии с ценностями и нормами, в том числе в онлайн-среде, чему способствуют разработка, реализация и участие в различных социальных проектах, а также в других видах деятельности, предлагаемых в рамках курса. Обучающиеся осознают смысл овладения цифровыми технологиями.

Формируются также готовность и способность к участию в различных видах онлайн-деятельности, направленных на личностное развитие; осознанное стремление соответствовать социально одобряемым нормам поведения по отношению к взрослым и сверстникам в различных онлайн-контекстах. У детей появляется потребность участвовать в онлайн-деятельности, способствующей личностному развитию. Во время изучения курса «Информационная безопасность» формируются *ИКТ-компетенции*: умение строить поисковые запросы в онлайн-источниках и находить релевантную информацию; умение анализировать, сопоставлять, обобщать, интерпретировать и систематизировать информацию, оценивать её достоверность; умение сохранять и передавать информацию, в том числе в форме гипермедиа (текст, изображение, звук, ссылки между разными информационными компонентами), при соблюдении правил кибербезопасности. Приобретённые компетенции позволят более эффективно осваивать программы других курсов.

Раздел II. «Организационно-педагогические условия»

2.1 Календарный учебный график программы (Приложение №1)

Место проведения занятий – кабинет проектной деятельности МАОУ СОШ №10.

Время проведения – согласно расписанию.

2.2. Условия реализации программы

Учебно-методическое и материально-техническое обеспечение образовательной деятельности.

В учебно-методический комплекс для изучения программы «Информационнаябезопасность» входят программа, методическое пособие, учебник, электронная форма учебника для воспроизведения на электронных устройствах (компьютерах, планшетах, в том числе с подключением к интерактивной доске) для каждой группы. Электронные формы учебников созданы на основе печатных версий учебников. Для полноценной реализации программы необходим соответствующий аудиторный фонд с оборудованием, позволяющим реализовывать различные виды деятельности, включая расходные материалы и канцелярские принадлежности, а также мебель, компьютерное оснащение, презентационное оборудование. В аудитории созданы условия для проведения индивидуальной и групповой работы. Уроки, требующие использования Интернета, обеспечены индивидуальными цифровыми устройствами для учащихся в зависимости от заданий (смартфон, компьютер/ноутбук, планшет) и высокоскоростным, устойчивым доступом к сети Интернет.

Нормативно-правовая база курса

1. Федеральный закон от 29 декабря 2012 г. № 273-ФЗ «Об образовании в Российской Федерации».
2. Федеральный государственный образовательный стандарт основного общего образования (утв. приказом Министерства просвещения РФ от 31 мая 2021 г. № 287).
3. Федеральный закон от 27 июля 2006 г. № 149-ФЗ «Об информации, информационных технологиях и о защите информации».
4. Федеральный закон от 27 июля 2006 г. № 152-ФЗ «О персональных данных».
5. Федеральный закон от 29 декабря 2010 г. № 436-ФЗ «О защите детей от информации, причиняющей вред их здоровью и развитию».
6. Указ Президента Российской Федерации от 29 мая 2017 г. № 240 «Об объявлении в Российской Федерации Десятилетия детства».
7. Указ Президента Российской Федерации от 1 декабря 2016 г. № 642 «О Стратегии научно-технологического развития Российской Федерации».
8. Указ Президента РФ от 9 мая 2017 г. № 203 «О Стратегии развития информационного общества в Российской Федерации на 2017–2030 гг.».

Литература

Основная литература

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). 15

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%20 ReportRussian.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/2017cifrovoe_ 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 А. А., 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.

10. Методическое пособие к учебнику Г. У. Солдатовой, С. В. Чигарьковой «Кибербезопасность» для 5-9 классов общеобразовательных организаций / авт.-сост. Г. У. Солдатова, С. В. Чигарькова. — М.: ООО «Русское слово — учебник», 2022. — 144 с. — (ФГОС)

11. Учебник Г. У. Солдатовой, С. В. Чигарьковой «Кибербезопасность» для 5-9 классов общеобразовательных организаций / авт.-сост. Г. У. Солдатова, С. В. Чигарькова. — М.: ООО «Русское слово — учебник», 2022. — 144 с. — (ФГОС)

Интернет-ресурсы

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).

2.3. Форма аттестации

Объединение «Информационная безопасность» предполагает различные виды и формы контроляпромежуточных и итоговых результатов освоения образовательной программы.

Задачи контроля:

- определение фактического состояния учащегося в данный момент времени;
- определение причин выявленных отклонений от заданных предметов;
- обеспечение устойчивого состояния учащегося.

Виды контроля:

- начальная диагностика;
- текущий контроль;
- итоговая аттестация.

Формы проведения итогов реализации образовательной программы:

- педагогическое наблюдение за каждым учащимся;
- опрос;
- рефлексия;
- защита проектов;
- участие в конкурсах.

Методом контроля и управления учебного процесса является анализ результатов конкурсов, выполнение творческих заданий, а также наблюдение педагога в ходе занятий, подготовки, участие в мероприятиях различного уровня.

Проследить динамику развития знаний, умений и действий поможет диагностика. Начальная диагностика проводится для выявления уровня знаний учащихся в области кибербезопасности.

С целью определения степени усвоения учащимися учебного материала проводится текущий контроль (педагогическое наблюдение, опрос, рефлексия).

С целью определения изменения уровня развития детей, их творческих способностей на конец срока реализации программы проводится итоговая аттестация (защита творческих проектов с занесением результатов мониторинга в протокол аттестации учащихся).

Система оценивания результатов аттестации учащихся: высокий уровень; средний уровень; низкий уровень.

2.4. Оценочные материалы

№	Фамилия, имя учащегося	Умение распознавать опасности в сети	знание основ кибербезопасности	креативность
1				
2				
3				
4 …				

Оценивается в баллах:

1 - низкий уровень

2 - средний

3 – высокий

Низкий уровень	Учащиеся пишут распознают угрозы с помощью советов, используют небезопасные пароли, опасаются общаться в сети.
Средний уровень	Учащиеся распознают не все угрозы в сети, умеют обеспечивать безопасность паролей и интернет-соединений, допускают небезопасное поведение в сети
Высокий уровень	Учащиеся легко и быстро распознают угрозы в сети, умеют организовать безопасное индивидуальное интернет-пространство, пользуются правилами общения в сети и соблюдают этикет