

Муниципальное общеобразовательное учреждение
«Средняя общеобразовательная школа № 2 г. Ершова Саратовской области
им. Героя Советского Союза Зуева М.А.»

ПРИНЯТА

на заседании
педагогического совета
МОУ «СОШ № 2 г. Ершова
Саратовской области им. Героя
Советского Союза Зуева М.А.»

Протокол № 13 от «03» мая 2024 г.

УТВЕРЖДАЮ

Директор
МОУ «СОШ № 2 г. Ершова
Саратовской области им.
Героя Советского Союза
Зуева М.А.»

Тихова Ю.А.

Приказ № 161 от «07» мая 2024 г.



**ДОПОЛНИТЕЛЬНАЯ ОБЩЕОБРАЗОВАТЕЛЬНАЯ
ОБЩЕРАЗВИВАЮЩАЯ ПРОГРАММА
социально- гуманитарной направленности**

«Информационная безопасность»

Возраст обучающихся: 9-11 лет
Срок реализации программы: 1 год

Автор-составитель:
Капулова Людмила Режебовна,
педагог дополнительного образования

г. Ершов, 2024 г.

I. «Комплекс основных характеристик дополнительной общеобразовательной общеразвивающей программы»

Пояснительная записка

Дополнительная общеобразовательная программа «Информационная безопасность» разработана в связи с возросшей потребностью обеспечения информационной безопасности детей и подростков при организации урочной и внеурочной деятельности.

Дополнительная общеобразовательная общеразвивающая программа «**Информационная безопасность**» МОУ «СОШ №2 г. Ершова Саратовской области» им. Героя Советского Союза Зуева М.А. разработана в соответствии с:

- «Законом об образовании в Российской Федерации» (№273-ФЗ от 29 декабря 2012 г.);
- «Порядком организации и осуществления образовательной деятельности по дополнительным общеобразовательным программам» (пр. Министерства образования и науки РФ от 27 июля 2022 г. №629)
- Приказом Министерства образования и науки Российской Федерации от 23 августа 2017 года №816 «Об утверждении Порядка применения организациями, осуществляющими образовательную деятельность, электронного обучения, дистанционных образовательных технологий при реализации образовательных программ»;
- Постановлением Главного государственного санитарного врача РФ от 28 сентября 2020 года №28 «Об утверждении СанПиН 2.4.4.3648-20 «Санитарно-эпидемиологические требования к организациям воспитания и обучения, отдыха и оздоровления детей и молодежи»;
- Положением о дополнительной общеобразовательной общеразвивающей программе МОУ «СОШ №2 г. Ершова Саратовской области» им. Героя Советского Союза Зуева М.А.

Программа реализуется в **очной форме с использованием электронных (дистанционных) форм**. В связи с тем, что в течение учебного года возникает непреодолимая сила, или форс- мажор – обстоятельства (эпидемия, карантин, погодные условия и прочее), не позволяющие осуществлять обучение в обычной (очной) форме, программа реализуется с помощью электронных (дистанционных) технологий.

Направленность дополнительной общеобразовательной программы - социально-гуманитарная.

Актуальность. Исследование проблемы безопасности детей и подростков в сети Интернет последние годы является особенно актуальным, в связи с бурным развитием IT-технологий и со свободным использованием детьми и подростками современных информационно – коммуникационных технологий (Интернет, сотовая (мобильная) связь).

Новизна программы состоит в том, что рассматриваются вопросы информационной безопасности, которая является одной из составляющих безопасности личности, а также вопросы информационной культуры личности, которая способствует реальному пониманию человеком самого себя, своего места и роли в окружающем мире.

Программа «Информационная безопасность» разработана для расширения кругозора и формирования мировоззрения учащихся, повышения уровня безопасности человека в окружающей его информационной среде.

Педагогическая целесообразность определена тем, что ориентирует на приобщение каждого ребенка к информационной науке. Позволяет применить полученные знания, умения и навыки кибербезопасности в повседневной деятельности, улучшить образовательный результат, в области информатики. Благодаря обучению по данной программе обучающиеся приобретают общую информационную культуру. Кроме того, педагогическая целесообразность образовательной программы основывается на формировании у обучающегося чувства ответственности в выполнении своей индивидуальной, так и групповой работе.

Адресат, возрастные особенности обучающихся.

Младший школьный возраст 7-10 лет. В этом возрасте дети располагают значительными резервами развития. Их выявление и эффективное использование – одна из главных задач возрастной и педагогической психологии. Общими характеристиками всех познавательных процессов ребенка становятся их произвольность, продуктивность и устойчивость. Для того, чтобы умело использовать имеющиеся у ребенка резервы, необходимо как можно быстрее адаптировать детей к работе в школе и дома, научить их учиться, быть внимательным, усидчивым. Младший школьный возраст является периодом интенсивного развития и качественного преобразования познавательных процессов: они начинают приобретать опосредствованный характер и становятся осознанными и произвольными. Ребенок постепенно овладевает своими психическими процессами, учится управлять восприятием, вниманием, памятью. Подвижность, любознательность, конкретность мышления, большая впечатлительность, подражательность и вместе с тем неумение долго концентрировать свое внимание на чем-либо, характерные черты данной возрастной категории.

Средний школьный возраст 11-14 лет — самый благоприятный для творческого развития. В этом возрасте обучающимся нравится решать проблемные ситуации, находить сходство и различие, определять причину и следствие. Им нравится высказать свое мнение и суждение. Самому решать проблему, участвовать в дискуссии, отстаивать и доказывать свою правоту. Исследования внутреннего мира подростков показывают, что одной из самых главных моральных проблем среднего школьного возраста является несогласованность убеждений, нравственных идей и понятий с поступками, действиями, поведением. Система оценочных суждений, нравственных идеалов неустойчива. Особое значение для подростка в этом возрасте имеет возможность самовыражения и самореализации. Обучающимся будет интересна деятельность, которая служит активному самовыражению подростков и учитывает их интересы.

Объем и срок освоения программы: Общее количество часов – 36 (18 часов - 3 кл, 18 часов - 4 кл). Продолжительность занятий исчисляется в академических часах- 45 минут. Занятия проводятся 1 раз в неделю.

Особенности организации образовательного процесса. Образовательный процесс организован в соответствии с индивидуальным учебным планом в объединении, являющихся основным составом кружка. Состав группы постоянный. Программа предусматривает индивидуальные, групповые, фронтальные формы работы с детьми.

Цель и задачи программы

Цель программы: освоение обучающимися базовых принципов безопасного поведения в сети интернет и безопасности личного информационного пространства.

Задачи обучения:

Образовательные:

1. Способствовать формированию знаний о безопасном поведении при работе с компьютерными программами, информацией в сети Интернет;
2. Формировать умения соблюдать нормы информационной этики;
3. Формировать умения безопасной работы с информацией, анализировать и обобщать полученную информацию.

Развивающие:

1. Развивать компьютерную грамотность информационную культуру личности в использовании информационных и коммуникационных технологий;
2. Развивать умение анализировать и систематизировать имеющуюся информацию;
3. Развивать познавательную и творческую активность в безопасном использовании информационных и коммуникационных технологий;

Воспитательные:

1. Способствовать выработке сознательного и бережного отношения к вопросам собственной информационной безопасности;

2. Способствовать формированию и развитию нравственных, этических, патриотических качеств личности.
3. Стимулировать поведение и деятельность, направленные на соблюдение информационной безопасности.

Планируемые результаты:

Предметные:

1. Сформированы знания о безопасном поведении при работе с компьютером;
2. Сформированы умения соблюдать нормы информационной этики;
3. Сформированы умения безопасно работать с информацией, анализировать и обобщать полученную информацию.

Метапредметные:

1. Развита компьютерная грамотность и информационная культура личности в использовании информационных и коммуникационных технологий;
2. Развита способность анализировать и систематизировать имеющуюся информацию;
3. Развита познавательная и творческая активность в безопасном использовании информационных и коммуникационных технологий.

Личностные:

1. Выработано сознательное и бережное отношение к вопросам собственной информационной безопасности;
2. Сформированы и развиты нравственные, этические, патриотические качества личности;
3. Сформировано поведение и деятельность, направленные на соблюдение информационной безопасности.

Содержание программы
Учебный план дополнительной общеобразовательной общеразвивающей программы
«Информационная безопасность»
3 класс

№ п/п	Тема	Всего часов	Теоретические занятия	Практические занятия	Формы контроля
1.	Вводное занятие. Информация, компьютер и Интернет.	4	3	1	Тестирование/онлайн тестирование Практикум/онлайн-практикум
2.	Техника безопасности и экология	3	2	1	Практикум/онлайн-практикум
3.	Мир виртуальный и реальный. Интернет зависимость.	3	2	1	Практикум/онлайн-практикум Квест/онлайн-квест
4.	Методы безопасной работы в Интернете	3	2	1	Исследование/онлайн-исследование
5.	Потребительские опасности в Интернете	2	1	1	Квест/онлайн-квест
6.	Основные правила поведения сетевого взаимодействия	2	1	1	Практикум/онлайн-практикум
7.	Государственная политика в области защиты информации	1	1	0	Тестирование/онлайн-тестирование
	Итого	18	12	6	

4 класс

№п/п	Тема	Всего часов	Теоретические занятия	Практические занятия	Формы контроля
1	Вводное занятие. Общие сведения о безопасности Интернета	4	3	1	Тестирование/онлайн тестирование Практикум/онлайн-практикум
2	Техника безопасности и экология	3	2	1	Практикум/онлайн-практикум
3	Проблемы Интернет - зависимости	3	2	1	Практикум/онлайн-практикум
4	Методы обеспечения безопасности и Интернета. Вирусы и антивирусы.	3	2	1	Практикум/онлайн-практикум
5	Мошеннические действия в Интернете. Киберпреступления	2	1	1	Практикум/онлайн-практикум
6	Сетевой этикет. Психология и сеть	2	1	1	Практикум/онлайн-практикум
7	Государственная политика в области кибербезопасности	1	1	0	Тестирование/онлайн-тестирование
	Итого:	18	28	8	

Содержание учебного плана 3 класс

Тема №1.-4ч.

Информация, компьютер и Интернет.

- 1. Теория: Вводное занятие.** Компьютер — как он появился, как появился Интернет. Почему компьютер нужно беречь. Где и как искать информацию для занятия. Интернет –средство для поиска полезной информации. Как защитить себя от информационной перегрузки. Что такое файл. Как обращаться со своими и чужими файлами, чтобы их не потерять. Какие файлы можно скачивать, а какие нельзя. Полезные и вредные страницы Интернета. Как отличать полезную и правдивую информацию. Ненужные ссылки, ложные ссылки, реклама. Что такое вредоносные сайты. К чему ведет переход по вредоносным ссылкам. Опасная информация в сети. Возьми с собой электронного помощника. Мобильные устройства. Польза и опасности мобильной связи, Общение в Интернете переписка, форумы, социальные сети. Совместные игры в Интернете. Обмен данными при совместной работе скайп, Ф-телефония, ICQ. Безопасный обмен данными. На каких устройствах можно сохранить информацию и как с ними правильно обращаться (диски, флэш, карты и пр.). Как работать в группе. Как передать товарищам результаты работы и не повредить их компьютерам. Что такое электронная почта.
- 2. Практика: Практическая работа №1. Поиск информации в сети Интернет. Общение с использованием видеосвязи на примере Skype. Создание электронной почты.**

Тема №2.-3ч.

Техника безопасности и экология

- 1. Теория:** Гигиена при работе с компьютером. Правила работы с ПК, электронными книгами и мобильными устройствами. Сколько времени можно проводить за компьютером. Как правильно сидеть за компьютером. Как защитить компьютер от повреждений, Компьютеру тоже нужна забота, Компьютер и среда обитания (растения, животные, другие члены семьи). Везде ли есть Интернет? Может ли компьютер заменить компас. Как мобильные устройства помогают ориентироваться на местности. Воздействие компьютера на зрение и др. органы. Физическое и психическое здоровье. Польза и вред компьютерных игр. Компьютер и недостаток движения. Что делать с компьютером в чрезвычайных ситуациях. Улица и мобильные устройства. Компьютер (мобильные устройства) в грозу.
Практика: Практическая работа №1.Создание буклетов по темам (на выбор):
 - «Как может помочь компьютер в сложных чрезвычайных ситуациях»
 - «Правила поведения на улице с мобильными устройствами»
 - «Компьютеру тоже нужна забота»(как ухаживать за ПК и мобильными устройствами)

Тема №3.-3ч.

Мир виртуальный и реальный. Интернетзависимость.

- 1. Теория:** Что такое Интернет-сообщество. Как не превратить свою жизнь в виртуальную? Социальные сети. Детские социальные сети. Какую информацию о себе следует выкладывать в сеть? Какая информация принадлежит вам? Не слишком ли много у вас друзей в социальной сети? Если слишком долго находиться в Интернете: что такое интернет-зависимость? Виртуальная личность что это такое. Сайты знакомств. Незнакомцы в Интернете. Превращение виртуальных знакомых в реальных. Развлечения в Интернете. Игры полезные и вредные. Признаки игровой зависимости.

1. Практика:

Практическая работа №1. Тест «Есть у меня игровая зависимость». Квест «Я умею говорить «Нет» в сети интернет»

Тема №4.-3ч.

Методы безопасной работы в Интернете.

1. Теория: Ищите в Интернете только то, что вам требуется. Как защититься от вредного контента. Что такое контент-фильтры, движение в Интернете (серфинг). Знаки Интернета, рассказывающие об опасной информации. Правильно ли работает компьютер? Признаки работы вирусов. Вирусы и антивирусы. Почему родители проверяют, что ты делаешь в Интернете?

2. Практика:

Практическая работа №1. Исследовательская работа «Колобанга в поисках вируса» (выявление признаков заражения вирусом).

Тема №5.-2 ч.

Потребительские опасности в Интернете

1. Теория:

Интернет и экономика польза и опасность. Кто и как может навредить в Интернете. Электронная торговля ее опасности. Поиск информации: если у вас требуют личную информацию при скачивании данных. Что такое личная информация. Если вам сообщают о выигрыше в лотерею. Если вам предлагают установить новое приложение. Сколько стоят ошибки в интернете.

2. Практика: Практическая работа №1. Квест «Покупка в интернет-магазине».

Тема №6.-2ч.

Основные правила поведения сетевого взаимодействия.

1. Теория: Что такое интернет-этикет. Как вести себя в гостях у «сетевых» друзей.

2. Практика: Практическая работа №1.«Пишу письмо другу»

Тема №7.-1ч.

Государственная политика в области защиты информации.

1. Теория: Основные вопросы: Как государство защищает киберпространство. Почему государство защищает информацию.

Практика: Итоговое занятие. Тестирование. «Я и безопасность»

4 класс

Тема №1.(4ч)

Общие сведения о безопасности ПК и Интернета

1. Теория: Как устроены компьютер и интернет. Как работают мобильные устройства. Угрозы для мобильных устройств. Защита персональных данных, почему она нужна. Категории персональных данных. Биометрические персональные данные. Безопасный профиль в социальных сетях. Составление сети контактов. Защита киберпространства как комплекс мероприятий, направленных на обеспечение информационной безопасности. Аспекты кибербезопасности Компьютерная и информационная безопасность, обнаружение проблем сети, восстановление параметров систем, средства защиты от несанкционированного доступа к данным, криптографическая защита информации. Основные угрозы безопасности информации: утечки, потеря целостности, нарушение работоспособности системы, незаконное тиражирование (воспроизведение). Безопасный серфинг. Безопасные ресурсы для поиска.

2. Практика: Практическая работа. Составить информационный буклет «Моя безопасная сеть» или сделать групповую газету «Безопасность в Интернет».

Тема №2. (3ч)

Техника безопасности и экология

1. Теория: Правила поведения в компьютерном классе. Техника безопасности при работе с компьютером. Компьютер и мобильные устройства в чрезвычайных ситуациях. Компьютер и зрение. Воздействие радиоволн на здоровье и окружающую среду (Wi-Fi, Bluetooth, GSM). Комплекс упражнений при работе за компьютером. Гигиена при работе с ПК

Практика:

Практическая работа. Создание буклета «Техника безопасности при работе с компьютером».

Тема №3.(3ч)

Проблемы Интернет-зависимости

1. Теория: ЗОЖ и компьютер. Деструктивная информация в Интернете - как ее избежать. Психологическое воздействие информации на человека. Управление личностью через сеть. Интернет и компьютерная зависимость (аддикция). Критерии зависимости с точки зрения психологов (приоритетность, изменения настроения, толерантность, симптом разрыва, конфликт, рецидив). Как развивается зависимость. Типы интернет - зависимости (пристрастие к работе с компьютером, к навигации и поиску информации, игромания и электронные покупки, зависимость от сетевого общения, сексуальные зависимости).

2. Практика:

Практическая работа. «Создание мультимедийной презентации «ПК и ЗОЖ. Организация рабочего места».

Тема №4.(3ч)

Методы обеспечения безопасности ПК и Интернета. Вирусы и антивирусы.

1. Теория: Вирусы человека и компьютера, цели компьютерных вирусов. Типы вирусов. Отличия вирусов и закладок. Как распространяются вирусы. Что такое антивирусная защита. Как лечить компьютер. Антивирусные программы для ПК: сканеры, ревизоры и др. Выявление неизвестных вирусов. Защита мобильных устройств. Безопасность при скачивании файлов. Защита программ и данных от несанкционированного копирования. Организационные, юридические, программные и программно-аппаратные меры защиты. Защита программ и данных с помощью паролей, программных и электронных ключей, серийных номеров, переноса в онлайн и т.п. Методы защиты фото и видеоматериалов от копирования в сети. Проверка подлинности (аутентификация) в Интернете. Меры личной безопасности при сетевом общении. Настройки приватности в социальных сетях. Предотвращение несанкционированного доступа к ПК. Пароли, биометрические методы защиты и аутентификация с помощью внешних носителей.

2. Практика:

Практическая работа №1. Создание презентации на тему (по выбору): «Разновидности вирусов. Черви, трояны, скрипты», «Шпионские программы». «Шифровальщики». «Троян-вымогатель в социальной сети «ВКонтакте» или наказание для особо любопытных».

Тема №5.(2ч)

Мошеннические действия в Интернете. Киберпреступления.

1. Теория: Виды интернет - мошенничества (письма, реклама, охота за личными данными и т.п.). Фишинг (фарминг). Мошеннические действия в сети. Предложения о разблокировании программ (блокировщики windows). Ложные антивирусы. Сбор «пожертвований» на благотворительность. «Легкий заработок» в Интернете. Пирамиды. Мошенничество при распространении «бесплатного» ПО. Продажа «обучающих курсов» для бизнеса. Опасности мобильной связи. Предложения по установке вредоносных приложений. Мошеннические СМС. Прослушивание разговоров. Определение местоположения телефона. Азартные игры. Онлайн-казино. Букмекерские конторы. Предложения для «инвестирования» денег. Выигрыш в лотерею. Технологии манипулирования в Интернете.

Техника безопасности при интернет-общении.

2. Практика:

Практическая работа. Доклад на тему: «Правила поведения в сети с мошенниками и злоумышленниками», или «Как не стать жертвой сетевых шуток и розыгрышей».

Тема №6.(2ч)

Сетевой этикет. Психология и сеть

1. Теория: Что такое этикет. Виды этикета (личный, деловой, письменный, дискуссионный и пр.). Различия этикета в разных странах. Как появился этикет, что это такое. Сетевой этикет. Общие правила сетевого этикета. Этика дискуссий. Взаимное уважение при интернет-общении. Этикет и безопасность. Эмоции в сети, их выражение. Примеры этических нарушений. Безопасная работа в сети в процессе сетевой коммуникации (чаты, форумы, конференции, скайп, социальные сети и пр.). Термины сетевого этикета: оверквотинг, флейм, флуд, оффтопик, смайлики и др. Психологическая обстановка в Интернете: грифинг, кибербуллинг, кибер-моббинг, троллинг, буллицид. Если вы стали жертвой компьютерной агрессии: службы помощи личное общение и общение в группе - чем они отличаются (чаты, форумы, службы мгновенных сообщений)

3. Практика:

Практическая работа. «Выпуск видеоролика на тему «Как не испортить себе настроение при общении в Сети и не опуститься до уровня «веб-агрессора»».

Тема №7.(1ч)

Государственная политика в области кибербезопасности.

1. Теория: Собственность в Интернете. Авторское право. Интеллектуальная собственность. Платная и бесплатная информация. Защита прав потребителей при использовании услуг Интернет. Защита прав потребителей услуг провайдера. Как расследуются преступления в сети. Ответственность за интернет-мошенничество. Правовые акты в области информационных технологий и защиты киберпространства. Доктрина информационной безопасности.

2. Практика: Итоговое занятие. Тестирование. «Я и безопасность»

1.5. Формы контроля и их периодичность

Входной контроль проводится в начале учебного года, для определения уровня знаний и умений обучающихся на начало обучения по Программе. Оценка знаний учащихся осуществляется в ходе проведения тестирования.

Текущий контроль ведется на каждом занятии в форме педагогического наблюдения за правильностью выполнения практической работы; аттестация обучающихся осуществляется в ходе анкетирования, тестирования, квеста, практикума и др.

Промежуточный контроль проводится по итогам изучения каждого раздела Программы в форме выполнения творческого задания. Аттестация проводится в форме практикума.

Итоговый контроль проводится на последнем итоговом занятии в конце мая. Аттестация осуществляется в форме тестирования.

Метапредметные и личностные результаты.

Текущий контроль проводится с использованием метода педагогического наблюдения в ходе осуществления творческой деятельности.

Раздел №2. «Комплекс организационно-педагогических условий»

Методическое обеспечение программы Образовательный процесс по дополнительной общеобразовательной общеразвивающей программе «Информационная безопасность» реализуется в очной форме с использованием электронных (дистанционных) технологий.

Программа предполагает сочетание коллективных, групповых, индивидуальных форм организации и форм **наставничества** на занятиях. Коллективные задания вводятся в программу с целью формирования опыта общения и чувства коллективизма.

Программа направлена на освоение обучающимися правил безопасного поведения в нестандартных ситуациях, а также предполагает получение знаний о личной безопасности в цифровой среде.

В ходе реализации программы возможно использование различных **методов и приёмов** организации занятий:

- По источнику получения информации — практический (опыты, упражнения); наглядный (иллюстрация, демонстрация, наблюдения обучающихся); словесный (объяснение, разъяснение, рассказ, беседа, инструктаж, лекция, дискуссия, диспут); работа с книгой (чтение, изучение, реферирование, цитирование, беглый просмотр, конспектирование); видеометод (просмотр, обучение, упражнение, контроль);
- По характеру дидактической цели — приобретение знаний; формирование умений и навыков; применение знаний; формирование творческой деятельности; закрепление и контроль знаний, умений, навыков;
- По характеру познавательной деятельности — поисковые; объяснительно-иллюстративные; репродуктивные; проблемного изложения; эвристические (частично-поисковые); исследовательские;
- по соответствию методов обучения логике общественно-исторического познания — организация наблюдения, накопление эмпирического материала; обобщение теоретической обработки фактических данных; практическая проверка правильности выводов и обобщений, выявление истины, соответствия содержания и формы, явления и сущности;
- по соответствию методов обучения специфике изучаемого материала и форм мышления — научного познания реальной действительности; освоения искусства; практического применения знаний.

Все эти методы и приёмы направлены на стимулирование познавательного интереса обучающихся и формирование творческих учений и навыков.

Формы проведения учебных занятий подбираются с учетом цели и задач, специфики содержания данной общеобразовательной программы и возраста обучающихся. Программой предусмотрены групповые и индивидуальные формы занятий, **электронная (дистанционная) формы**, а также занятие-беседа, занятие-викторина и т.д.

Формы взаимодействия субъектов образовательного процесса в случае электронного обучения с применением дистанционных технологий предусматривается взаимодействие с педагогом, обучающимися, родителями – помощниками в техническом обеспечении образовательного процесса.

Формы организации учебного занятия:

3 класс

В разделе 1 предполагается изучение понятий Информация, компьютер и Интернет; во 2 разделе предполагается изучение знаний технике безопасности и экологии; в 3 разделе предполагается изучение виртуального мира и как не стать интернет-зависимым;

в 4 разделе предполагается формирование знаний о методах безопасной работы в Интернете; в 5 разделе предполагается изучение потребительских опасностей в Интернете;

в разделе изучаются основные правила поведения сетевого взаимодействия;

в 7 разделе знакомятся с государственной политикой в области защиты информации подводятся итоги полученных навыков и знаний по информационной безопасности.

4 класс

в разделе 1 предполагается изучение сведений о безопасности Интернета;

в разделе 2 предполагается изучение знаний техники безопасности и экологии;

в разделе 3 предполагается знакомство с проблемами интернет - зависимости;

в разделе 4 предполагается изучение методов обеспечения безопасности ПК и Интернета;

в разделе 5 предполагается формирование знаний о мошеннических действиях в Интернете и киберпреступлениях;

в разделе 6 изучается сетевой этикет;

в разделе 7 знакомятся с государственной политикой в области кибербезопасности и подводятся итоги полученных навыков и знаний по информационной безопасности.

Главное условие успешного обучения – это способность педагога постоянно совершенствовать занятие, находить новые подходы, **приемы обучения** обучающихся, это - создание ситуации успеха, использование дифференцированного и индивидуального подходов, возможность поделиться своими достижениями и успехами, возможность каждого обучающегося видеть своё движение вперёд, педагогическое сотрудничество и др.

Педагогические технологии, используемые в представлении программного материала

№	Наименование технологии, методик	Характеристика технологий в рамках образовательной программы
1	Технология группового обучения	С помощью групповой технологии учебная группа, поделённая на подгруппы, решает и выполняет конкретные задачи таким образом, что виден вклад каждого обучающегося.
2	Технология исследовательской деятельности	Способствует созданию проблемных ситуаций и активной деятельности обучающихся по их разрешению, в результате происходит поиск интересного материала.
3	Игровая технология	Обеспечивает личностную мотивационную включённость каждого обучающегося, что значительно повышает результативность обучения по программе
4	Здоровьесберегающая технология	Благодаря этим технологиям обучающиеся учатся жить вместе и эффективно взаимодействовать. Они способствуют активному участию самого обучающегося в освоении культуры человеческих отношений, в формировании опыта здоровьесбережения, который приобретается через постепенное расширение сферы общения и деятельности ребёнка, становления самосознания и активной жизненной позиции на основе воспитания и самовоспитания, формирования ответственности за своё здоровье, жизнь и здоровье своих товарищей.
5	Электронные (дистанционные) технологии	С помощью этих процессов происходит подготовка и передача информации обучающемуся, через компьютер (дистанционно)

Условия реализации программы

Материально-технические условия реализации программы включает следующий перечень необходимого оборудования:

1. Компьютер;
2. Мультимедийный проектор.
3. Интерактивная доска

4. Доступ к сети Интернет.

Информационное обеспечение реализации программы

Для реализации программы используются следующие методические материалы: календарный график; методическая литература для педагогов дополнительного образования и обучающихся; ресурсы информационных сетей по методике проведения занятий

Интернетресурсы:

Полезные ссылки для педагога:

- 1) <http://www.kaspersky.ru>—антивирус«ЛабораторияКасперского»;
- 2) <http://www.onlandia.org.ua/rus/>-безопаснаяweb-зона;
- 3) <http://www.interneshka.net> международный онлайн-конкурс по безопасному использованию Интернета;
- 4) Рыжков В.Н. Методика преподавания информатики// <http://nto.immdu.sya.ru/sites/default/files/3/12697.vdf>;
- 5) <http://www.saferinternet.ru> — портал Российского Оргкомитета по безопасному использованию Интернета;
- 6) <http://content-filterind.ru>—ИнтернетСМИ«ВашличныйИнтернет»;
- 7) <http://www.rddb.ru>—Российскаягосударственнаядетскаябиблиотека
- 8) <http://www.saferinternet.ru/>- Безопасный Интернет. Портал Российского Оргкомитета по проведению Года Безопасного Интернета. Мероприятия, Интернет и законодательство, проблемы и решения, международные ресурсы;
- 9) <http://www.saferunet.ru/>- Центр Безопасного Интернета в России. Сайт посвящен проблеме безопасной, корректной и комфортной работы в Интернете. Интернет-угрозы и эффективное противодействие им в отношении пользователей;
- 10) <http://www.fid.su/>- Фонд развития Интернет. Информация о проектах, конкурсах, конференциях и др. по компьютерной безопасности и безопасности Интернета;
- 11) <http://www.microsoft.com/Rus/athome/security/kids/etusivu.html>Безопасность в Интернете. "Основы безопасности детей и молодежи в 30 Интернете" —интерактивный курс по Интернет-безопасности, предлагаемый российским офисом Microsoft в рамках глобальной инициативы Microsoft "Безопасность детей в Интернете" и "Партнерство в образовании". В разделе для учащихся (7-16 лет) предлагается изучить проблемы информационной безопасности посредством рассказов в картинках. В разделе для родителей и учителей содержится обновленная информация о том, как сделать Интернет для детей более безопасным, а также изложены проблемы компьютерной безопасности;
- 12) <http://www.ifab.ru>

Кадровое обеспечение

Реализацию дополнительной общеобразовательной общеразвивающей программы «Информационная безопасность» осуществляет педагог дополнительного образования с высшим образованием, первой квалификационной категорией

2.4 Оценочные материалы

Критерии оценки предметных результатов по разделам (темам) и планируемых оцениваемых параметров метапредметных и личностных результатов дополнительной общеобразовательной общеразвивающей программы «Информационная безопасность» в рамках входящего, текущего контроля, промежуточной/ итоговой аттестации:

Показатели (оцениваемые параметры)	Степень выраженности оцениваемого качества	Число баллов	Мет оды диагно стики
Образовательные результаты			
Теоретические знания по разделам/темам учебно-	овладел менее чем 1/2 объема знаний, предусмотренных программой	1	Наблюдение, тестирование и
тематического плана программы	объем усвоенных знаний составляет более 1/2	2	др.
	освоил практически весь объем знаний, предусмотренных программой за конкретный период	3	
Практические умения и навыки, предусмотренные программой	овладел менее чем 1/2 предусмотренных умений и навыков	1	Наблюдение, защита исследовательской работы, мини-проекта
	объем усвоенных умений и навыков составляет более 1/2	2	
	овладел умениями и навыками, предусмотренными программой за конкретный период	3	
Личностные результаты			
Сформированность активности, организаторских способностей	мало активен, наблюдает за деятельностью других, забывает выполнить задание. Результативность невысокая	1	Наблюдение, тестирование и др.
	активен, проявляет стойкий познавательный интерес, трудолюбив, добивается хороших результатов	2	
	активен, проявляет стойкий познавательный интерес, добивается выдающихся результатов, инициативен, организует деятельность других	3	
Сформированность коммуникативных навыков, коллективизма	поддерживает контакты избирательно, чаще работает индивидуально, публично не выступает	1	Наблюдение, тестирование и др.
	вступает и поддерживает контакты, не вступает в конфликты, дружелюбен со всеми, по инициативе руководителя или группы выступает перед аудиторией	2	
	легко вступает и поддерживает контакты, разрешает конфликты, дружелюбен со всеми, инициативен, пособственному желанию успешно выступает перед аудиторией	3	

Сформированность ответственности, самостоятельности, дисциплинированности	неохотно выполняет поручения. Начинает работу, но часто не доводит ее до конца.	1	Тестирование, наблюдение.
	справляется с поручениями и соблюдает правила поведения только при наличии контроля и требовательности преподавателя; выполняет поручения охотно, ответственно. Хорошо ведет себя независимо от наличия или отсутствия контроля, но не требует этого от других	2	
	выполняет поручения охотно, ответственно, часто по собственному желанию, может привлечь других. Всегда дисциплинирован, везде соблюдает правила поведения, требует того же от других	3	
Сформированность креативности, склонности к самостоятельному творчеству, исследовательско- проектной деятельности	может работать в проектно-исследовательской группе при постоянной поддержке и контроле. Способен принимать творческие решения, в основном использует традиционные способы	1	Тестирование, наблюдение.
	может разработать свой творческий проект с помощью педагога. Способен на творческие решения, в основном использует традиционные способы	2	
	высокий творческий потенциал. Самостоятельно выполняет работы. Является разработчиком творческих проектов. Находит нестандартные решения, новые способы выполнения заданий	3	
Метапредметные результаты			
Понимать и принимать учебную задачу, сформулированную педагогом	овладел менее чем 1/2 объема задач, предусмотренных программой	1	Тестирование, наблюдение.
	объем усвоенных задач составляет более 1/2	2	
	демонстрирует полное понимание, предусмотренных программой задач за конкретный период	3	
Проявлять индивидуальные творческие способности	знает отдельные специальные навыки, но избегает их употреблять	1	Тестирование, наблюдение.
	сочетает специальную навыки с бытовыми	2	
	проявляет творческие способности осознанно и в полном соответствии с их содержанием	3	

Планировать свои действия на отдельных этапах работы над выполнением творческого задания	овладел менее чем 1/2 объема знаний, предусмотренных программой	1	Тестирование, наблюдение.
	демонстрирует неполное освоение планируемых действий, но более 1/2	2	
	освоил план действий в заданных условиях	3	
Осуществлять контроль, коррекцию и оценку результатов своей деятельности; понимать и применять полученную информацию при выполнении заданий	знает, но избегает их употреблять в деятельности	1	Тестирование, наблюдение.
	демонстрирует неполное освоение заданных параметров, но более 1/2	2	
	освоил план действий в заданных условиях	3	

Тест по безопасности в сети Интернет (3 класс)

1. Как могут распространяться компьютерные вирусы?
 - a. Посредством электронной почты.
 - б. При просмотре веб-страниц.
 - с. Через клавиатуру.
 - d. Их распространяют только преступники.
2. Зачем нужен брандмауэр?
 - a. Он не дает незнакомцам проникать в компьютер и просматривать файлы.
 - б. Он защищает компьютер от вирусов.
 - с. Он обеспечивает защиту секретных документов.
 - d. Он защищает компьютер от пожара.
3. Всегда ли можно быть уверенным в том, что электронное письмо было получено от указанного отправителя?
 - a. Да
 - б. Да, если вы знаете от отправителя
 - с. Нет, поскольку данные от отправителя можно легко подделать
 - d. Может быть.
4. На компьютере отображается непонятное сообщение. Какое действие предпринять?
 - a. Продолжить. Будто ничего не произошло.
 - б. Нажать кнопку «ОК» или «ДА»
 - с. Обратиться за советом к учителю, родителю или опекуну.
 - d. Больше никогда не пользоваться Интернетом
5. Что нужно сделать при получении подозрительного сообщения электронной почтой?
 - a. Удалить его, не открывая.
 - б. Открыть его и выяснить, содержится ли в нем какая-нибудь важная информация.
 - с. Открыть вложение, если такое имеется в сообщении.
 - d. Отправить его родителям
6. В ящик входящей почты пришло «письмо счастья». В письме говорится, чтобы его переслали пяти друзьям. Какое действие предпринять?
 - a. Переслать его пяти друзьям.
 - б. Переслать его не пяти друзьям, а десяти друзьям.
 - с. Не пересылать никакие «письма счастья»
 - d. Ответить отправителю, что вы больше не хотите получать от него/нее письма.
7. В каких случаях можно, не опасаясь последствий, сообщать в Интернет свой номер телефона или домашний адрес?
 - a. Во всех случаях.
 - б. Когда кто-то просит об этом.
 - с. Когда собеседник в чате просит об этом.
 - d. Такую информацию следует с осторожностью сообщать людям, которым вы доверяете.
8. Вы случайно прочитали пароль, который ваш друг записал на листочке бумаги. Как вы должны поступить?
 - a. Запомнить его.
 - б. Постараться забыть пароль.
 - с. Сообщить другу, что вы прочитали пароль, и посоветовать сменить пароль и никогда больше не записывать на листе бумаги.
 - d. Сообщить пароль родителям.
9. Что такое сетевой этикет?

- a. Правила поведения за столом.
- б. Правила дорожного движения.
- с. Правила поведения в Интернете.
- d. Закон, касающийся Интернета.

10. Что запрещено в интернете?

- a. Запугивание других пользователей
- б. Поиск информации.
- с. Игры.
- d. Общение с друзьями

Тест по безопасности в сети Интернет (4 класс)
«Основы безопасности в Интернете» Осторожно, вирус!

1. Что является основным каналом распространения компьютерных вирусов?
 - а. Веб- страницы
 - б. Электронная почта
 - с. Флеш-накопители (флешки)
2. Для предотвращения заражения компьютера вирусом следует:
 - а. Не пользоваться Интернетом
 - б. Устанавливать и обновлять антивирусные средства
 - с. Не чихать и не кашлять рядом с компьютером
3. Если вирус обнаружен, следует:
 - а. Удалить его и предотвратить дальнейшее заражение
 - б. Установить какую разновидность имеет вирус
 - с. Выяснить как он попал на компьютер
4. Что не дает хакерам проникать в компьютер и просматривать файлы и документы:
 - а. Применение брандмауэра
 - б. Обновления операционной системы.
 - с. Антивирусная программа
5. Какое незаконное действие преследуется в России согласно Уголовному Кодексу
 - а. Уничтожение компьютерных вирусов
 - б. Создание и распространение компьютерных вирусов вредоносных программ
 - с. Установка программного обеспечения для защиты компьютера

Осторожно, Интернет!

1. Какую информацию нельзя разглашать в Интернете?
 - а. Свои увлечения
 - б. Свой псевдоним.
 - с. Домашний адрес
2. Чем опасны социальные сети?
 - а. Личная информация может быть использована кем угодно в различных целях
 - б. При просмотре непознанных ссылок компьютер может быть взломан
 - с. Все вышеперечисленное верно
3. Виртуальный собеседник предлагает встретиться, как следует поступить?
 - а. Посоветоваться с родителем и ничего не предпринимать без их согласия
 - б. Пойти на встречу одному.
 - с. Пригласить с собой друга
4. Что в Интернете запрещено законом?
 - а. Размещать информацию о себе
 - б. Размещать информацию других без их согласия.
 - с. Копировать файлы для личного использования
5. Действуют ли правила этикета в Интернете?
 - а. Интернет-пространство свободное от правил
 - б. В особых случаях

с. Да, как в реальной жизни

Тест по безопасности в сети Интернет

1. Когда можно полностью доверять новым онлайн-друзьям?
 - a) Ничто не может дать 100%-ную гарантию того, что онлайн-другу можно доверять
 - b) Поговорив по телефону
 - c) После обмена фотографиями
 - d) Когда есть общие друзья
 - e) Последнего онлайн-знакомства (переписки)

2. Что делать, если ты столкнулся со странным в Сети?
 - a) Сообщить модераторам сайта
 - b) Рассказать взрослым
 - c) Игнорировать выпады тролля
 - d) Заблокировать тролля
 - e) Проучить или доказать свою правоту

3. Как пожаловаться на неприемлемый контент на YouTube?
 - a) Выразить свое недовольство в комментариях к видео
 - b) Отметить видео “флажком”, который находится под ним
 - c) Такого функционала нет
 - d) Найти электронный адрес автора видео и написать ему сообщение

4. Что является признаком фишинг-сообщения?
 - a) В сообщении много ошибок, неточностей и противоречий
 - b) Сообщение содержит обещание большой выгоды с минимальными усилиями
 - c) В сообщении требуется срочно сменить пароль от электронной почты по причине невероятной попытки взлома электронного ящика, при этом сообщение не отправлено с официального адреса почтовой службы
 - d) В сообщении запрашиваются твои личные данные, финансовая информация, пароли
 - e) Сообщение содержит угрозу для жизни и здоровья близких людей

5. Как обезопасить себя при первой встрече с онлайн-другом?
 - a) Заранее пообщаться с “незнакомцем” по телефону, попросить прислать фотографии, таким образом убедиться, что он тот, за кого себя выдает
 - b) Убедиться, что у вас есть общие увлечения и темы для разговора в реальной жизни
 - c) Встречаться с интернет-незнакомцами очень опасно, лучше не назначать встречу, если не знакомы с человеком лично
 - d) Попросить присутствовать взрослых
 - e) Сообщить о встрече родителям/взрослым, спросить их совета
 - f) Взять на встречу друзей и выбрать людное место в светлое время суток

6. Где можно найти информацию для реферата в Интернете?
 - a) На сайтах средств массовой информации
 - b) В электронной библиотеке
 - c) В поисковой системе
 - d) В Википедии

7. Какую информацию о себе опасно выкладывать в Интернете в открытом доступе? а) Дату рождения
б) Свои интересы
в) Информацию о доходах родителей
г) Домашний адрес и телефон
д) Место работы родителей
8. Как пожаловаться на неприемлемый контент на YouTube?
а) Отметить видео «флажком», который находится под ним
б) Такого функционала нет
в) Выразить свое недовольство в комментариях к видео
г) Найти электронный адрес автора видео и написать ему сообщение
9. Что делать, если вы стали жертвой интернет-мошенничества? а) Сообщить взрослым
б) Сменить все пароли
в) Попробовать решить проблему самостоятельно
г) Позвонить на Линию помощи «Дети онлайн»
10. Как нужно себя вести, если вы стали жертвой кибербуллинга? а) Обратиться за поддержкой к модераторам сайта
б) Пытаться бороться с обидчиком в одиночку
в) Заблокировать обидчика
г) Сообщить родителям/взрослым
д) Ничего не делать
е) Обратиться на Линию помощи «Дети онлайн»
11. Как защититься от негативного контента?
а) Установить программы родительского контроля
б) Сообщить модераторам сайта, пожаловаться на неприемлемый контент с помощью специальных инструментов, доступных на сайте
в) Обратиться к автору негативного контента
г) Не обращать на него внимания
д) Использовать безопасный поиск Google и безопасный режим на YouTube
12. Что следует делать, если на сайте вас спросят отправить бесплатное сообщение на короткий номер?
а) Как можно быстрее отправить СМС
б) Постараться узнать стоимость СМС на сайте, после этого поискать в интернете, какова стоимость отправки СМС на этот номер, и перепроверить эту информацию. До перепроверки информации не отправлять СМС
в) Использовать телефон друга или знакомого, чтобы отправить СМС
13. Что делать, если ты столкнулся с троллем в Сети? а) Игнорировать выпады тролля
б) Проучить или доказать свою правоту
в) Заблокировать тролля
г) Рассказать взрослым
д) Сообщить модераторам сайта
14. Как защитить свою электронную почту от взлома и атак? а) Регулярно

менять пароли

b) Активировать систему двухэтапной верификации на сервисах, которые позволяют это сделать

с) Никому не сообщать свой пароль

d) Периодически менять адрес электронной почты, менять провайдера

e) Не открывать сообщения с незнакомых и подозрительных адресов

f) Создавать разные пароли от разных аккаунтов, включая электронную почту, систему электронного банкинга и пр.

15. При каких условиях можно доверять письму от неизвестного отправителя? а) Никогда нельзя доверять письму от неизвестного отправителя

b) К вам обращаются по имени

с) Отправитель использует логотип авторитетной компании

d) Письмо содержит важную информацию о ваших близких

e) Отправитель ссылается на ваших друзей

16. Что делать, если вам пришло письмо отом, что вы выиграли в лотерею? а) Отметить сообщение как спам

b) Перейти по ссылке в письме, ведь в редких случаях информация может оказаться правдой

с) Удалить его

d) Заблокировать отправителя

e) Написать ответ разоблачающе письмо мошенникам

17. Что делать, если вам приходит сообщение по электронной почте или во всплывающих окнах о том, что ваш компьютер заражён?

a) Пройти по предлагаемым ссылкам и скачать антивирусную систему

b) Закрывать всплывающее окно и не нажимать на ссылки в нём

с) Просканировать компьютер на возможные вирусы, при этом не переходить по незнакомым ссылкам

18. Как защитить компьютер от вредоносных программ?

a) Никогда не переходить по ссылкам из всплывающих окон

b) Перед запуском проверять все файлы, скачанные из Интернета, с помощью антивируса

с) Регулярно обновлять браузер, операционную систему, антивирусную программу и прикладное программное обеспечение

d) Установить на компьютер сразу несколько антивирусных программ e) Установить антивирусную программу с официального сайта

f) Не открывать вложения в письмах, присланных с неизвестных электронных адресов, а также с осторожностью относиться к письмам, которые пришли с известного адреса, но чье содержание кажется подозрительным: аккаунт ваших знакомых может быть взломан и содержать вирусы

19. Какие функции браузера не следует использовать на общественном компьютере? а) Безопасный поиск

b) Автозаполнение форм

с) Автосохранение паролей

d) Режим инкогнито

20. В каком случае нарушается авторское право?

- a) При размещении на YouTube собственного видеоролика сконцерт любимой группы
- b) При использовании материалов Википедии для подготовки реферата с ссылкой на источник
- c) При размещении нелицензионного контента в социальных сетях
- d) При просмотре нелицензионного контента в социальных сетях
- e) При чтении романа Л.Н. Толстого «Война и мир» в Интернете

21. Что в Интернете запрещено законом?

- a) Размещать информацию о себе
- b) Размещать информацию других без их согласия
- c) Копировать файлы для личного использования

22. Действуют ли правила этикета в Интернете?

- a) Интернет-пространство свободно от правил
- b) В особых случаях
- c) Да, как в реальной жизни

23. Чем опасны социальные сети?

- a) Личная информация может быть использована кем угодно в различных целях
- b) При просмотре непознанных ссылок компьютер может быть взломан
- c) Все вышеперечисленное верно

24. Что не дает хакерам проникать в компьютер и просматривать файлы и документы:

- a) Применение брандмауэра
- b) Обновления операционной системы
- c) Антивирусная программа

25. Какое незаконное действие преследуется в России согласно Уголовному Кодексу

- a) Уничтожение компьютерных вирусов
- b) Создание и распространение компьютерных вирусов и вредоносных программ
- c) Установка программного обеспечения для защиты компьютера

2.5. Список литературы

Полезные ссылки для обучающихся:

- 1) <http://www.svmantec.com/ru/ru/nonon/clubsvmantec/library/article.isvaid=csteachkids>— ClubSvmantec единый источник сведений об безопасности в Интернете. Статья для родителей «Расскажите детям об безопасности в Интернете». Информация о средствах родительского контроля;
- 2) <http://www.nachalka.com/bezobasnost>-Nachalka.com предназначен для учителей, родителей, детей, имеющих отношения к начальной школе. Статья «Безопасность детей в Интернете». Советы учителями родителям;
- 3) <http://www.obzh.info/novosti/novoe/bezobasnost-detei-v-internete.html> Личная безопасность. Основы безопасности жизни. Рекомендации и в зрелом: как сделать посещение Интернета для детей полностью безопасным;
- 4) <http://www.ifao.ru/library/book099.odf>-«Безопасность детей в Интернете», компания Microsoft. Информация для родителей: памятки, советы, рекомендации;
- 5) http://www.interneshka.net/children/index_dhtml - «Интернешка» - детский онлайн-конкурс по безопасному использованию сети Интернет. Советы детям, педагогам и родителям, «полезные ссылки». Регистрация и участие в конкурсе по безопасному использованию сети Интернет;
- 6) <http://www.oszone.net/6213/> - OS.zone.net - Компьютерный Инфо-журнал ИИНОРТАЛ. Статьи для родителей «Обеспечение безопасности детей при работе в Тернет». Рекомендации и программы «Родительский КОНТРОЛЬ»;
- 7) <http://www.rydb.ru/innocuous-internet/> - Российская государственная детская библиотека. Ресурс для детей и родителей. Правила безопасного Интернета. Обзор программных продуктов для безопасного Интернета. Как защитить компьютер от угроз. Ссылки на электронные ресурсы, информирующие об опасностях и защите в сети;
- 8) <https://www.yooyale.ru/safetvcenter/families/stan/basics/> - Центр безопасности. Как защитить ребенка и помочь обеспечить безопасность членов семьи в Тернете, даже если вы не знаете времени;
- 9) <https://eяe.vandex.ru/security/>-Тест по безопасности;
- 10) <http://www.slideshare.net/shderk/ss-47136465>-Безопасность в Тернете. Анастасия Шперх;
- 11) <http://shberk.ru/v-seti/brokrustovo-lozhe.html> - Прохрустово ложь для Инфо-журнала ИИНОРТАЛ. Как мы читаем текст в Интернете;
- 12) <http://shderk.ru/sovetv/avtoritet.html>-Как отличить фейк от настоящего материала? Дело о лготе и мдьяхекрякутном;
- 13) <http://habrahabr.ru/comoanv/mailru/blos/252091/>-Советы по безопасности.
<http://www.ifav.ru>

Полезные ссылки для педагогов

1. Вы знаете, что делают ваши дети в Интернете?
<http://www.youtube.com/watch?v=d2OwtGPEdh4&feature=related>
2. Защищайте детей от Интернета
<http://www.youtube.com/watch?v=bdnXmTbZX04&feature=related>
3. ЛИНИЯ Помощи "Дети онлайн"
<http://www.youtube.com/watch?v=oivzlwJoxk4>

ПРОИЗВЕДено И
ПРОИЗМЕРено И
41 инст. 1055444
Директор МОУ «СОШ №2 г. Ермаова
Сапаринской области
И.И. Ермаова Советского Союза Звезда М.А.с
/Ю.А.Т./ (100000)

