Лоськов Сергей Евгеньевич

Подписано цифровой подписью: Лоськов Сергей Евгеньевич
Дата: 2022.06.15 08:37:36 +05'00'

ДЕПАРТАМЕНТ СОЦИАЛЬНОЙ ПОЛИТИКИ
МУНИЦИПАЛЬНОЕ БЮДЖЕТНОЕ ОБЩЕОБРАЗОВАТЕЛЬНОЕ УЧРЕЖДЕНИЕ ГОРОДА КУРГАНА
«СРЕДНЯЯ ОБЩЕОБРАЗОВАТЕЛЬНАЯ ШКОЛА № 23»

Принята на заседании
методического совета
от «12» мая 2022г.
протокол № 4__

Утверждаю:
Директор МБУО «СОШ№23»
_____ Лоськов С.Е.
приказ от «_12_» мая 2022 г.
№ 94/1___

Дополнительная общеобразовательная (общеразвивающая) программа социально-гуманитарной направленности

«Цифровой мир и мы»

Возраст обучающихся: 11-16 лет

Срок реализации: 1 год

Автор-составитель: Попова Анастасия Анатольевна,
педагог дополнительного образования

г. Курган, 2021г.

1.Комплекс основных характеристик программы

Направленность программы	социально-гуманитарная
Актуальность программы	Исследование проблем безопасности детей и подростков в сети Интернет, в связи с бурным развитием IT-технологий и со свободным использованием детьми и подростками современных информационно - коммуникационных технологий (Интернет, сотовая (мобильная) связь).
Отличительные особенности программы	Способствует разностороннему раскрытию индивидуальных способностей учащихся, развитию у них интереса к различным видам деятельности, желанию активно участвовать в практической деятельности, умению самостоятельно организовывать свое свободное время.
Адресат программы	Требования к уровню подготовки учащихся Знать/понимать: - об истории появления компьютера и Интернета.; правила работы с компьютером; технические и программные возможности мобильных устройств; преимущества мобильной связи и их опасность; соблюдать правила работы с файлами; отличать безопасные сайты и ссылки от вредоносных; понимать пользу и опасности виртуального общения, социальных сетей; - основные правила работы с ПК, электронными книгами и мобильными устройствами в условиях окружающей среды, основные навыки ухода за ПК, опасности при работе с электрическими приборами; - виды общения в Интернете; правила безопасной работы при интернет – общении; чего не следует делать при сетевом общении; - основные понятия о компьютерных вирусах и контент-фильтрах; - принципы работы интернет - магазинов, понятие «электронные деньги»; - правила сетевого этикета; - политику государство в области защиты информации. Уметь: - правильно работать за компьютером; пользоваться браузером для поиска полезной информации; внимательно прочитывать сообщения о нежелательных страницах, отказываться от их просмотра; выполнять основные действия с файлами; копировать файлы, проверять

	файлы на вирусы; работать с информацией и электронной почтой; владеть основными приемами поиска информации в сети Интернет; - соблюдать технику безопасности и гигиену при работе за ПК; владеть основными приемами навигации в файловой системе; - пользоваться основными видами программ для общения в сети; - отличать вредные игры от полезных; - использовать приемы работы с антивирусными программами, запускать программы-антивируса для сканирования компьютера и внешних носителей информации, устанавливать и сканировать антивирусной программой; - дозировано использовать личную информацию в сети интернет; различать (распознавать) мошеннические действия; - корректно общаться в сети Интернет; - защищать свои информационные данные от внешнего воздействия (интернет и вирусы, вирусы и злоумышленники).
Срок реализации (освоения) программы	Срок реализации 1 год.
Объем программы	Рассчитана на 34 часа, 1 час в неделю.
Формы обучения, особенности организации образовательного процесса	Занятия проводятся в комбинированной, теоретической и практической форме: - теоретические занятия: основы безопасного поведения при работе с компьютерными программами, информацией в сети интернет, изучение терминов, беседы, лекции; - практические занятия: работа с мобильными устройствами; закупки в интернет магазине; квесты; создание буклетов и мультимедийных презентаций Содержание программного материала как в теории, так и на практических занятиях составлено с учётом возрастных особенностей обучающихся, весь материал построен по принципу от простого к сложному. Практические работы в содержании программы возможно использовать в качестве вариативных, индивидуальных практических заданий разного уровня углубленности, доступности и степени сложности исходя из диагностики и стартовых возможностей каждого из участников рассматриваемой программы.

Уровни сложности содержания программы	Стартовый (ознакомительный) - 1 год

1.2. Цели и задачи программы. Планируемые результаты

Цель и задачи программы, планируемые результаты	Цель программы: освоение обучающимися базовых принципов безопасного поведения в сети Интернет и безопасности личного информационного пространства. Задачи обучения: Обучающие: 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; Воспитывающие: 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. Результаты освоения программы «Цифровой мир и мы»: Личностные: 1. Вырабатывается сознательное и бережное отношение к вопросам собственной информационной безопасности; 2. Формируются и развиваются нравственные, этические, патриотические качества

	личности; 3. Стимулируется поведение и деятельность, направленные на соблюдение информационной безопасности. Метапредметные: 1. Развиваются компьютерная грамотность и информационная культура личности в использовании информационных и коммуникационных технологий; 2. Развиваются умения анализировать и систематизировать имеющуюся информацию; 3. Развиваются познавательная и творческая активность в безопасном использовании информационных и коммуникационных технологий.
1.1. Рабочая программа	
Учебный план. Содержание программы. Тематическое планирование	

Учебный план

Учебный план для программы «Цифровой мир им ы» сроком реализации 1 год

№ п/п	Название раздела программы	Количество часов			Формы промежуточной аттестации
		всего	теория	практика	
1.	Информация, компьютер и Интернет	8	6	2	
2.	Техника безопасности и экология	8	5	3	
3.	Мир виртуальный и реальный. Интернет зависимость.	5	3	2	
4.	Методы безопасной работы в Интернете	5	3	2	
5.	Потребительские опасности в Интернете	4	3	1	
6.	Основные правила поведения сетевого взаимодействия	2	1	1	
7.	Государственная политика в области в защиты информации	2	1	1	
9.	Промежуточная аттестация				Выставка работ обучающихся
	Итого	34	22	12	

Содержание программы	Раздел 1. Информация, компьютер и Интернет.(8 часов) Компьютер - как он появился, как появился Интернет. Почему компьютер нужно беречь. Где и как искать информацию для урока. 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, IP-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. Раздел 2. Техника безопасности и экология. (8 часов) 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. Раздел 3. Мир виртуальный и реальный. Интернет зависимость. (5 часов) 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.

<table>
<tr><td></td><td>Раздел 4. Методы безопасной работы в Интернете. (5 часов)
Ищите в Интернете только то, что вам требует 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. Обновление баз. Что такое электронные деньги, как с ними правильно обращаться. Почему родители проверяют, что ты делаешь в Интернете?
Раздел 5. Потребительские опасности в Интернете. (4 часа)
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.
Раздел 6. Основные правила поведения сетевого взаимодействия. (2 часа)
Что такое интернет-этикет. Как вести себя в гостях у «сетевых» друзей.
Раздел 7. Государственная политика в области защиты информации. (2 часа)
Основные вопросы: Как государство защищает киберпространство. Войны нашего времени. Что такое кибервойна. Почему государство защищает информацию. Защита государства и защита киберпространства.</td></tr>
<tr><td>Тематическое планирование</td><td>тематическое планирование

1-й год обучения
<table>
<tr><th>№ п/п</th><th>Название раздела программы</th><th>Дата проведения занятия</th><th>Кол-во часов</th><th>Тема занятия</th><th>Форма занятия</th><th>Форма текущего контроля / промежуточной аттестации</th></tr>
<tr><td>1</td><td>Информация, компьютер и Интернет</td><td>02.09</td><td>1</td><td>Компьютер - как он появился, как появился Интернет.</td><td>Беседа. Вводный инструктаж на рабочем месте</td><td></td></tr>
</table></td></tr>
</table>

		2	Информация, компьютер и Интернет	09.09.	1	Интернет средство для поиска полезной информации.	Беседа. Практическая работа	
		3	Информация, компьютер и Интернет	16.09	1	Как защитить себя от информационной перегрузки.	Беседа	
		4	Информация, компьютер и Интернет	23.09	1	Полезные и вредные страницы Интернета.	Беседа	
		5	Информация, компьютер и Интернет	30.09	1	Что такое вредоносные сайты.	Беседа	
		6	Информация, компьютер и Интернет	07.10	1	Мобильные устройства. Польза и опасности мобильной связи.	Беседа	
		7	Информация, компьютер и Интернет	14.10	1	Безопасный обмен данными.	Беседа. Практическая работа	
		8	Информация, компьютер и Интернет	21.10	1	Что такое электронная почта.	Беседа	
		9	Техника безопасности и экология	11.11	1	Воспитание ценностных ориентиров на здоровый образ жизни	рассказ - беседа	
		10	Техника безопасности и экология	18.11	1	Воспитание ценностных ориентиров на здоровый образ жизни	рассказ – беседа, практическая работа	

		11	Техника безопасности и экология	25.11	1	Воспитывать творческую самостоятельность и инициативность	рассказ - беседа	
		12	Техника безопасности и экология	02.12	1	Воспитание нормы поведения в обществе	Дискуссия, практическая работа	
		13	Техника безопасности и экология	09.12	1	Воспитание ценностных ориентиров на здоровый образ жизни	дискуссия	
		14	Техника безопасности и экология	16.12.	1	Воспитание ценностных ориентиров на здоровый образ жизни	Дискуссия, практическая работа	
		15	Техника безопасности и экология	23.12	1	Воспитание нормы поведения в обществе	рассказ - беседа	
		16	Техника безопасности и экология	13.01	1	Воспитание ценностных ориентиров на здоровый образ жизни	дискуссия	
		17	Мир виртуальный и реальный. Интернет зависимость.	20.01	1	Воспитание взаимопонимания и уважения между учениками	Беседа, практическая работа	
		18	Мир виртуальный и реальный. Интернет зависимость.	27.01	1	Воспитание взаимопонимания и уважения между учениками	беседа	

		19	Мир виртуальный и реальный. Интернет зависимость.	03.02.	1	Воспитывать творческую самостоятельность и инициативно сть	беседа	
		20	Мир виртуальный и реальный. Интернет зависимость.	10.02	1	Воспитание ценностных ориентиров на здоровый образ жизни	дискуссия	
		21	Мир виртуальный и реальный. Интернет зависимость.	17.02	1	Воспитание ценностных ориентиров на здоровый образ жизни	Дискуссия, практическая работа	
		22	Методы безопасной работы в Интернете	24.02	1	Что такое контент-фильтры, движение в Интернете (серфинг).	дискуссия	
		23	Методы безопасной работы в Интернете	02.03	1	Знаки Интернета, рассказывающие об опасной информации.	Дискуссия, практическая работа	
		24	Методы безопасной работы в Интернете	09.03	1	Вирусы и антивирусы.	Беседа, практическая работа	
		25	Методы безопасной работы в	16.03	1	Что такое электронные деньги, как с ними правильно обращаться.	дискуссия	

	Интернете					
26	Методы безопасной работы в Интернете	01.04	1	Почему родители проверяют, что ты делаешь в Интернете?	дискуссия	
27	Потребительские опасности в Интернете	06.04	1	Интернет и экономика - польза и опасность.	дискуссия	
28	Потребительские опасности в Интернете	13.04	1	Электронная торговля - ее опасности.	Дискуссия, практическая работа	
29	Потребительские опасности в Интернете	20.04	1	Что такое личная информация	дискуссия	
30	Потребительские опасности в Интернете	27.04	1	Сколько стоят ошибки в интернете.	беседа	
31	Основные правила поведения сетевого взаимодействия	04.05	1	Что такое интернет-этикет.	беседа	
32	Основные правила поведения сетевого взаимодействия	11.05	1	Как вести себя в гостях у «сетевых» друзей.	Беседа, практическая работа	

		33	Государственная политика в области защиты информации.	18.05	1	Что такое кибервойна?	Дискуссия, практическая работа	
		34	Государственная политика в области защиты информации.	25.05	1	Почему государство защищает информацию.	беседа	

2 Комплекс организационно-педагогических условий

Календарный учебный график	**Календарный учебный график** Количество учебных недель: 34 недели Первое полугодие: с 01.09.2022 г. по 29.12.2022 г., 16 учебных недель Каникулы: с 30.12.2022 г. по 09.01.2023 г. Второе полугодие: с 10.01.2032 по 28.05.2023 г., 18 учебных недель Промежуточная аттестация: 20.05.2023 г.
Формы текущего контроля/ промежуточной аттестации	Формы подведения итогов реализации программы - выставки буклетов, выполненных обучающимися; проведение квестов; выступления обучающихся по актуальным вопросам информационной безопасности с собственными мультимедийными презентациями на ученических мероприятиях; демонстрация созданных видеороликов и др.

Материально-техническое обеспечение	Универсальный портативный компьютер, мультимедийный проектор, интерактивная доска, доступ к сети Интернет.
Информационное обеспечение	Видеофильмы, видеоролики социальной рекламы по безопасности в сети Интернет. 2ГИС, Госуслуги, социальные сети
Кадровое обеспечение	Профессиональный стандарт «Педагог дополнительного образования детей и взрослых», утвержденного приказом Министерства труда и социальной защиты РФ от 5 мая 2018 г. № 298н к образованию и обучению (направление подготовки, освоение программ профессиональной переподготовки и пр.).
Методические материалы	Формы реализации методов: •Объяснительно – иллюстративный метод предполагает изложение материала с применением картинок, схем, фотографий. •Образно – ассоциативный метод реализуется в форме рассказа- визуализации с примерами наиболее характерными для данной темы. •Демонстрационный метод реализуется в форме показа презентаций, фильмов-анимаций, учебных фильмов и т.д. •Типовая ситуация – метод, реализующийся в форме выполнения задания, изученного ранее и его анализ. •Инструктаж – метод реализуется в форме показа технологических карт, объяснения алгоритмов и правил работы в кабинете, с художественными материалами и оборудованием, объяснение правил ТБ и ОТ. •Практический метод – реализуется в форме конкурсов, выставок. •Технология проектного обучения – самостоятельная поисковая, исследовательская, проблемная, творческая деятельность обучающихся, совместная или индивидуальная. Программа предполагает создание обучающимися мини-проектов, отличием которых является решения какой-то небольшой проблемы.
Оценочные материалы	Тест по безопасности в сети интернет, с учетом разных возрастных групп
Список литературы	- Бирюков А.А. Информационная безопасность защита и нападение 2- е издание: Издательство:

	ДМК-Пресс., 2017, 434 с. - Бирюков А.А. Информационная безопасность защита и нападение.: Издательство: ДМК-Пресс., 2012, 474 с. - Колесниченко Денис. Анонимность и безопасность в интернете. От чайника к пользователю. Самоучитель Издательство: БХВ-Петербург, 2012, 240с. - Мазаник Сергей. Безопасность компьютера. Защита от сбоев, вирусов и неисправностей: издательство: ЭКСМО, 2014, 256 с. - Мэйволд Э. Безопасность сетей (2-е изд.) Книги» Сетевые Технологии. Название: Безопасностьсетей: Издательство: М.: НОУ "Интуит", 2016,571 с. - Платонов В.В. Программно-аппаратные средства защитыинформации: учебник для студ. Учрежд.высш.проф. образования / В. В.Платонов. — М.: Издательский центр «Академия», 2013, 336 с. - Проскурин В.Г Защита в операционных системах: Издательство: Горячая линия-Телеком, 2014, 192 с. - Савченко Е. Кто, как и зачем следит за вами через интернет: Москва - Третий Рим, 2012, 100 с. - Яковлев В.А.Шпионские и антишпионские штучки: Техническая литература Издательство: Наука и Техника, 2015, 320 с.
Приложение	Тест по безопасности в сети Интернет (начальное общее образование) 1. Как могут распространятся компьютерные вирусы? a. Посредством электронной почты. b. При просмотре веб-страниц. c. Через клавиатуру. d. Их распространяют только преступники. 2. Зачем нужен брандмауэр? a. Он не дает незнакомцам проникать в компьютер и просматривать файлы. b. Он защищает компьютер от вирусов. c. 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 b. Да, если вы знаете отправителя c. Нет, поскольку данные отправителя можно легко подделать d. Может быть. 4. На компьютере отображается непонятное сообщение. Какое действие предпринять? a. Продолжить Будто ничего не произошло. b. Нажать кнопку «ОК» или «ДА» c. Обратится 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. b. Открыть его и выяснить, содержится ли в нем какая-нибудь важная информация. c. 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. b. Переслать его не пяти друзьям, а десяти друзьям. c. 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 Интернете свой номер телефона или домашний адрес? a. Во всех случаях. b. Когда кто-то просит об этом. c. 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 бумаг. Как

	вы должны поступить? a. Запомнить его. b. Постараться забыть пароль. c. 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. b. Правила дорожного движения. c. Правила поведения в Интернете. d. Закон, касающийся Интернета. 10. Что запрещено в интернете? a. Запугивание других пользователей. b. Поиск информации. c. Игры. d. Общение с друзьями Тест по безопасности в сети Интернет (основное общее образование) «Основы безопасности в Интернете» Осторожно, вирус! 1. Что является основным каналом распространения компьютерных вирусов? a. Веб-страницы b. Электронная почта c. Флеш-накопители (флешки) 2. Для предотвращения заражения компьютера вирусами следует: a. Не пользоваться Интернетом b. Устанавливать и обновлять антивирусные средства c. Не чихать и не кашлять рядом с компьютером 3. Если вирус обнаружен, следует: a. Удалить его и предотвратить дальнейшее заражение b. Установить какую разновидность имеет вирус c. Выяснить как он попал на компьютер 4. Что не дает хакерам проникать в компьютер и просматривать файлы и документы:

	a. Применение брандмауэра b. Обновления операционной системы c. Антивирусная программа 5. Какое незаконное действие преследуется в России согласно Уголовному Кодексу РФ? a. Уничтожение компьютерных вирусов b. Создание и распространение компьютерных вирусов и вредоносных программ c. Установка программного обеспечения для защиты компьютера Осторожно, Интернет! 1. Какую информацию нельзя разглашать в Интернете? a. Свои увлечения b. Свой псевдоним c. Домашний адрес 2. Чем опасны социальные сети? a. Личная информация может быть использована кем угодно в разных целях b. При просмотре неопознанных ссылок компьютер может быть взломан c. Все вышеперечисленное верно 3. Виртуальный собеседник предлагает встретиться, как следует поступить? a. Посоветоваться с родителями и ничего не предпринимать без их согласия b. Пойти на встречу одному c. Пригласить с собой друга 4. Что в Интернете запрещено законом? a. Размещать информацию о себе d. Размещать информацию других без их согласия c. Копировать файлы для личного использования 5. Действуют ли правила этикета в Интернете? a. Интернет - пространство свободное от правил b. В особых случаях c. Да, как и в реальной жизни Тест по безопасности в сети Интернет

	(среднее общее образование) 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) После длительного онлайн-знакомства (переписки) 2. Что делать, если ты столкнулся с троллем 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 вероятной 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? a) Дату рождения b) О своих интересах c) Информацию о доходах родителей d) Домашний адрес и телефон e) Место работы родителей 8. Как пожаловаться на неприемлемый контент на YouTube? a) Отметить видео “флажком”, который находится под ним b) Такого функционала нет c) Выразить свое недовольство в комментариях к видео d) Найти электронный адрес автора видео и написать ему сообщение 9. Что делать, если вы стали жертвой интернет-мошенничества? a) Сообщить взрослым b) Сменить все пароли c) Попробовать решить проблему самостоятельно d) Позвонить на Линию помощи «Дети онлайн» 10. Как нужно себя вести, если вы стали жертвой кибербуллинга? a) Обратиться за поддержкой к модераторам сайта b) Пытаться бороться с обидчиками в одиночку c) Заблокировать обидчиков

	d) Сообщить родителям/взрослым e) Ничего не делать f) Обратиться на Линию помощи «Дети онлайн» 11. Как защититься от негативного контента? a) Установить программы родительского контроля b) Сообщить модераторам сайта, пожаловаться на неприемлемый контент с помощью специальных инструментов, доступных на сайте c) Обратиться к автору негативного контента d) Не обращать на него внимания e) Использовать безопасный поиск Google и безопасный режим на YouTube f) рос: 12. Что следует делать, если на сайте вас просят отправить бесплатное сообщение на короткий номер? a) Как можно быстрее отправить СМС b) Постараться найти 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 c) Использовать телефон друга или знакомого чтобы, отправить СМС 13. Что делать, если ты столкнулся с троллем в Сети? a) Игнорировать выпады тролля b) Проучить или доказать свою правоту c) Заблокировать тролля d) Рассказать взрослым e) Сообщить модераторам сайта 14. Как защитить свою электронную почту от взлома и махинаций? a) Регулярно менять пароли b) Активировать систему двухэтапной верификации на сервисах, которые позволяют это сделать c) Никому не сообщать свой пароль d) Периодически менять адрес электронной почты, менять провайдеров 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? a) Никогда нельзя доверять письму от неизвестного отправителя b) К вам обращаются по имени c) 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 о том, что вы выиграли в лотерее? a) Отметить сообщение как спам b) Перейти по ссылке в письме, ведь в редких случаях информация может оказаться правдой c) Удалить его d) Заблокировать отправителя e) Написать в ответ разоблачающее 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) Закрыть всплывающее окно и не нажимать на ссылки в нём c) Просканировать компьютер на возможные вирусы, при этом не переходить по незнакомым ссылкам 18. Как защитить компьютер от атак вредоносных программ? a) Никогда не переходить по ссылкам из всплывающих окон b) Перед запуском проверять все файлы, скачанные из Интернета, с помощью антивируса c) 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 вам 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? a) Безопасный поиск b) Автозаполнение форм c) Автосохранение паролей d) Режим инкогнито 20. В каком случае нарушается авторское право? a) При размещении на YouTube собственного видеоролика с концерта любимой группы b) При использовании материалов Википедии для подготовки реферата со ссылкой на источник c) При размещении не лицензионного контента в социальных сетях d) При просмотре не лицензионного 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 свободное от правил b) В особых случаях c) Да, как и в реальной жизни 23. Чем опасны социальные сети? a) Личная информация может быть использована кем угодно в разных целях b) При просмотре неопознанных 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

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