

**МУНИЦИПАЛЬНОЕ БЮДЖЕТНОЕ ОБЩЕОБРАЗОВАТЕЛЬНОЕ
УЧРЕЖДЕНИЕ «ГИМНАЗИЯ № 4 Г. УСТЬ-ДЖЕГУТЫ»**

СОГЛАСОВАНО МБОУ «Гимназия № 4 г. Усть-Джегуты» Руководитель Точки Роста Атабиева З.А.  30.08.2022 г.	УТВЕРЖДАЮ Директор МБОУ «Гимназия № 4 г. Усть-Джегуты»  А.М. Байкулова Приказ №562 31.08.2022 г.
---	--



РАБОЧАЯ ПРОГРАММА

Предметная область- информатика

Кибербезопасность

Класс – 7

Уровень образования - основное общее

Учебный год – 2022-2023

Срок реализации программы – 2022-2023 учебный год

Количество часов по учебному предмету - 1 час в неделю, всего – 34 часа в год

Рабочую программу составила: Шовгенова Анжела Мухамедовна

Год составления- 2022

**г. Усть-Джегута
2022**

Пояснительная записка

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).

Дополнительная общеобразовательная программа «Безопасность в сети Интернет» разработана в связи с возросшей потребностью обеспечения информационной безопасности детей и подростков при организации урочной и внеурочной деятельности. Программа разработана для следующих уровней общего образования: начального общего образования, основного общего и среднего общего образования.

Направленность дополнительной общеобразовательной программы - естественнонаучная.

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

В требованиях ФГОС к предметным результатам освоения курса информатики для уровней начального, основного общего и среднего общего образования отсутствует предметная область «Основы безопасности в Интернете», но в рамках метапредметных результатов и предметных умений дисциплины «Информатика» вопросы информационной безопасности обозначены.

Новизна дополнительной общеобразовательной программы «Безопасность в сети Интернет» заключается в достижении метапредметных результатов и предметных умений дисциплины «Информатика» по формированию навыков и умений безопасного и целесообразного поведения при работе с компьютерными программами и в сети интернет, умений соблюдать нормы информационной этики и права.

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.

Контингент обучаемых: программа рассчитана для обучающихся по трем уровням образования (начальное общее образование, основное общее образование, среднее общее образование). Объемом по 34 часов на каждый уровень образования соответственно.

Данная программа составлена на основе курса «Основы кибербезопасности» для общеобразовательных организаций авторов Тонких И.М., Комарова М.М., Ледовского В.И., Михайлова А.В., переработана и модифицирована.

Содержание программного материала этих тем, 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.

Планируемые результаты:

Предметные:

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

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.

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.

Режим занятий - занятия по данной программе могут проводиться один раз в неделю в рамках внеурочной деятельности в школе или в условиях учреждения дополнительного образования в соответствии с нормами СанПиН 2.4.2.2821-10 или СанПиН 2.4.4.3172-14.

Формы проведения занятий:

Формы организации деятельности: групповая, индивидуальная, индивидуально - групповая (3-5 человек). 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; покупки в интернет магазине; квесты; создание буклетов и мультимедийных презентаций.

Содержание курса

Тема 1. Общение в сети Интернет и сетевой этикет. (6 часов)

Основные вопросы: Почему соцсети стали настолько популярными? Механизмы

Интернет – общения. Графическая модель типов пользователей социальных сетей

Первая и главная причина – популяризация интернета. Именно с появлением подключения к Всемирной паутине в каждом доме соцсети стали одним из главных способов связи. Человечество всегда привлекала возможность коммуникации на расстоянии: телеграфы, телефоны, интернет.

Вторая причина – расширенный функционал. Социальные сети обладают не только возможностью переписываться и делиться новостями, но и:

- общаться по аудио- и видеосвязи;
- слушать музыку;
- смотреть фильмы, передачи, видео;
- делиться фотографиями;
- объединяться в сообщества по интересам;
- создавать коммерческие проекты и онлайн-представительства;
- вести бизнес, продавать товары и услуги;
- давать рекламу и многое другое.

Третья причина – [физиология человека](#).

Механизмы Интернет – общения.

Анонимность (человек в сети может проявлять и проявляет большую свободу высказываний и поступков (вплоть до нецензурных выражений), так как риск разоблачения минимален)

Своеобразие протекания процессов межличностного восприятия в условиях отсутствия невербальной информации (сильное влияние на представление о собеседнике имеют механизмы стереотипизации и идентификации, а также установка желаемых качеств в партнере)

Добровольность и желательность контактов (пользователь Интернета добровольно завязывает всевозможные контакты или уходит от них, а также может прервать их в любой момент)

Затрудненность эмоционального компонента общения (стойкое стремление к эмоциональному наполнению текста, которое выражается в создании смайликов для обозначения эмоций)

Стремление к ненормативному поведению (пользователи проигрывают нереализуемые в деятельности вне сети роли, сценарии ненормативного поведения).

Требования к знаниям и умениям:

Обучающиеся должны знать популяризация интернета. Почему соцсети стали настолько популярными? Механизмы Интернет – общения. Обучающиеся должны уметь различать графическая модель типов пользователей социальных сетей. Обучающиеся должны уметь использовать этические и правовые нормы информационной деятельности человека, информационный этикет и право, информационную безопасность

Тематика практических работ:

Практическая работа. Составить информационный буклет «Моя безопасная сеть», создать групповую газету «Безопасность в Интернет», «Упражнение Интернет общение глазами ребят».

Тема № 2. (5 часов) Риски в сети Интернет.

Основные вопросы: риски в сети Интернет.

Обучающиеся должны знать: Контентные риски. Различные информационные ресурсы (тексты, картинки, аудио, видеофайлы, ссылки на сторонние ресурсы), содержащие противозаконную, неэтичную и вредоносную информацию. Коммуникационные риски связаны с общением и межличностными отношениями Интернет-пользователей. Электронные риски – это вероятность столкнуться с хищением персональной информации

или подвергнуться атаке вредоносных программ. Потребительский риск заключается в потере денег без приобретения товара или приобретения товара низкого качества. Психологические риски интернет-зависимости.

Требования к знаниям и умениям:

Обучающиеся должны уметь различать риски в сети Интернет.

Тематика практических работ:

Практическая работа. Групповая работа «Риски в сети Интернет»

Создание буклета «Риски в сети Интернет».

Тема № 3. (3 часов)

Новостная грамотность в киберпространстве

Основные вопросы: Новостная грамотность. *Новость* - не жанр журналистского произведения, а новый фрагмент реальности, меняющий привычный ход вещей и потому требующий в той или иной степени общественного внимания. Виды новостей: «*Жесткая*» новость, «*Мягкая*» новость, *инфотейнмент*, *финишинг*. Главное, чтобы поднятая проблема была доведена до конца, закрыта в плане ее практического решения. Причем при использовании этого приема допускается повтор какой-то ситуации, факта, картинка, вопроса и т. д. Как оценить достоверность новостной информации? Как проверять информацию и не оказаться жертвой fake news? Принципы распознавания fake news. *Принцип первый:* проверьте площадку. *Принцип второй:* проверьте источники. *Принцип третий:* пускайте в свою голову только настоящих экспертов. *Принцип четвертый:* чем больше труда, тем лучше. *Принцип пятый:* ищите и распространяйте добавленную стоимость.

Требования к знаниям и умениям:

Обучающиеся должны знать новостную грамотность, виды новостей, как оценить достоверность новостной информации? Принципы распознавания fake news.

Тематика практических работ:

Практическая работа. «Создание мультимедийной презентации «Осторожно фейк!».

Тема № 4. (5 часов) Интернет зависимость

Основные вопросы: Термин "Интернет-зависимость" Термин "Интернет-зависимость" еще в 1996 году предложил доктор Айвен Голдберг для описания неоправданно долгого, возможно патологического, пребывания в Интернете. Виды интернет-зависимостей. Киберотношения. Зависимость от дружеских отношений, завязанных в комнатах общения, интерактивных играх и конференциях, которая заменяет реальных друзей и семью. Чрезмерная сетевая вовлеченность. Включает в себя вовлечение в азартные сетевые игры, зависимость от интерактивных аукционов и навязчивое состояние продавать и покупать через сеть. Информационная перегрузка и как ее опознать. Компьютерная зависимость. На сегодняшний день игровая зависимость официально признана врачами всего мира психическим заболеванием и включена в Международную классификацию болезней. Последствия компьютерной зависимости. *Физиологические проблемы:* Нарушение осанки; Рассеивается внимание; Снижаются умственные способности; Ухудшается память и зрение; Бессонница и потеря аппетита.

Требования к знаниям и умениям:

Обучающиеся должны знать виды интернет-зависимостей. Киберотношения. Информационная перегрузка и как ее опознать. Компьютерная зависимость и ее последствия.

Тематика практических работ:

Практическая работа. Создание презентации на тему: «Информационная перегрузка». Эссе «Я и Интернет»

Тема № 5. (5 часов)

Мошеннические действия в Интернете. Киберпреступления.

Основные вопросы: 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.

Требования к знаниям и умениям:

Обучающиеся должны знать: виды интернет-мошенничества, опасности мобильной сети, технику безопасности при регистрации на веб-сайтах, сайтах знакомств, понятия компьютерное пиратство, плагиат, кибернаемники и кибердетективы. Обучающиеся должны уметь обезопасить себя при интернет-общении.

Тематика практических работ:

Практическая работа. Круглый стол «Как не стать жертвой сетевых шуток и розыгрышей».

Тема № 6. (3 часа)

Агрессия в сети и ее виды

Основные вопросы: Термины «Агрессия и агрессивность»

Если вы стали жертвой компьютерной агрессии: службы помощи личное общение и общение в группе – чем они отличаются (чаты, форумы, службы мгновенных сообщений). Киберагрессия (оскорбление, унижение, манипуляция, буллинг в интернет-среде) — ситуация, в которую, по статистике, в России регулярно вовлекается каждый пятый подросток. С размытием границ реального и виртуального киберагрессия оказывает не менее пагубное влияние на эмоциональное и психологическое здоровье детей, чем реальная травля в школе (и одно нередко перетекает в другое). Кибербуллинг. Признаки кибербуллинга – осознанное и длительное причинение человеку вреда в сети. При этом агрессоров может быть несколько, они выступают как от своего лица, так и анонимно.

Требования к знаниям и умениям:

Обучающиеся должны знать термины «Агрессия и агрессивность». Кибербуллинг. Признаки кибербуллинга. Обучающиеся должны уметь использовать этические и правовые нормы информационной деятельности человека.

Тематика практических работ:

Практическая работа. Рисунок «Моя киберагрессия»

Тема №7. (3 часов)

Троллинг в киберпространстве

Основные вопросы: Троллинг — форма социальной провокации или издевательства в сетевом общении, использующаяся как персонифицированными участниками, заинтересованными в большей узнаваемости, публичности, эпатаже, так и анонимными пользователями. Виды троллинга: обычная провокация; преднамеренная провокация; целенаправленная провокация; троллинг по заказу. Типы троллей: эмоциональный тролль; тролль-оффтопикт; тролль-борец за справедливость; тролль — любитель спойлеров; тролли-всезнайки; «Бессмысленные» тролли.; «Актуальные» тролли; жестокие тролли.

Требования к знаниям и умениям:

Обучающиеся должны знать термин «Троллинг», его виды и типы. Обучающиеся должны уметь распознать троллинг и его виды в сети Интернет.

Тематика практических работ:

Практическая работа Буклет «[Не кормите Провокатора. Тролли в Интернете](#)»

Тема №8. (3 часов)**Хейтинг: способы нейтрализации**

Основные вопросы: Хейтинг — это такой вид социальной активности. Хейтерами обычно называют людей, которые по злому насмеваются или поливают грязью в интернете. Злые комменты, едкие выражения в адрес кого-либо. На этом многие даже себе сделали имя. Некоторые хейтеры причисляют себя к критикам, но критика по крайней мере имеет какой-то конструктив. Виды хейтеров: «Правдурб»; «Белое пальто»; «Троль обыкновенный»; «Эффект Шарикова». Если вы понимаете мотивы поведения хейтера, то вы можете защищаться и атаковать его.

Требования к знаниям и умениям:

Обучающиеся должны знать термин «Хейтинг», его виды. Обучающиеся должны уметь распознать хейтинг и его виды в сети Интернет.

Тематика практических работ:

Практическая работа. Создание презентации на тему: «Хейтинг: способы нейтрализации».

Учебно-тематический план

№ п/п	Наименование раздела, тем	Количество часов	Из них	
			теория	практика
1	Общение в сети Интернет и сетевой этикет	6	3	3
2	Риски в сети Интернет	5	2	3
3	Новостная грамотность в киберпространстве.	3	2	1
4	Интернет – зависимость	5	3	2
5	Мошеннические действия в Интернете. Киберпреступления	5	4	1
6	Агрессия в сети и ее виды	3	2	1
7.	Троллинг в киберпространстве	3	2	1
8.	Хейтинг: способы нейтрализации	3	2	1
9.	Итоговое занятие.	1	1	
Итого:		34	21	13

Раздел 4. Календарно-тематический план

№ п/п	Название темы	Кол-во часов		Формы организации познавательной деятельности учащихся	Планируемые результаты	Виды/ формы контроля
		Теор.	Прак.			
1. Общение в сети Интернет и сетевой этикет (6 часов)						
1	Социальные сети	1		Лекция.	Формирование знаний о безопасном поведении при работе скомпьютерными программами, информацией в сети интернет.	Текущий. Устный опрос.
2	Механизмы Интернет - общения	1		Лекция.	Формирование знаний о безопасном поведении при работе скомпьютерными программами, информацией в сети интернет.	Текущий. Устный опрос.
3	Практическая работа «Информационный буклет «Моя безопасная сеть»		1	Рассказ-беседа.	Развитие умение анализировать и систематизировать имеющуюся информацию.	Текущий. Индивидуальная работа.
4	Графическая модель типов пользователей социальных сетей	1		Беседа.	Стимулирование поведение я деятельности, направленные на соблюдениеинформационной безопасности	Текущий. Фронтальный опрос.
5	Практическая работа «Информационная газета «Безопасность в Интернет»		1	Практическая работа.	Развитие умения анализировать и систематизировать имеющуюся информацию.	Текущий. Групповая работа.
6	Упражнение «Интернет		1	Лекция.	Формирование знаний о	Текущий.

	общение глазами ребят». Тест «Сетевой этикет»				безопасном поведении при работе с компьютерными программами, информацией в сети интернет.	Устный опрос.
2.Риски в сети Интернет (5 часов)						
7,8	Контентные и коммуникационные риски в сети Интернет. Практическая работа.	1	1	Практическая работа.	Развитие сознательного и бережного отношения к вопросам собственной информационной безопасности.	Текущий. Устный опрос.
9,10	Электронные и потребительские риски в сети Интернет. Практическая работа.	1	1	Практическая работа.	Формирование умения соблюдать нормы информационной этики.	Текущий. Устный опрос.
11	Психологические риски интернет- зависимости. Блиц-опрос «Я и моя информационная безопасность»		1	Практическая работа.	Развитие познавательной и творческой активности в безопасном использовании информационных и коммуникационных технологий.	Текущий. Уплотнённый опрос.
3.Новостная грамотность в киберпространстве (3 часа)						
12	Новостная грамотность. Виды новостей	1		Лекция.	Стимулирование поведения и деятельности, направленных на соблюдение информационной безопасности.	Текущий. Устный опрос
13	Принципы распознавания fake news. Как оценить достоверность новостной информации?	1		Рассказ-беседа.	Развитие компьютерной грамотности и информационной культуры личности в использовании информационных и коммуникационных технологий.	Текущий. Устный опрос

14	Практическая работа. Создание презентации «Осторожно fake news»		1	Практическая работа.	Развитие познавательной и творческой активности в безопасном использовании информационных и коммуникационных технологий.	Текущий. Групповая работа.
4.Интернет – зависимость (5 часов)						
15	Виды Интернет – зависимостей. Киберотношения.	1		Лекция.	Стимулирование поведения и деятельности, направленных на соблюдение информационной безопасности.	Текущий. Устный опрос.
16	Информационная перегрузка. Как опознать информационную перегрузку.	1		Беседа.	Развитие компьютерной грамотности и информационной культуры личности в использовании информационных и коммуникационных технологий.	Текущий. Устный опрос.
17	Практическая работа. Создание презентации «Информационная перегрузка»		1	Практическая работа.	Развитие познавательной и творческой активности в безопасном использовании информационных и коммуникационных технологий.	Текущий. Работа в парах.
18	Компьютерная зависимость. Её последствия.	1		Лекция.	Развитие сознательного и бережного отношения к вопросам собственного здоровья.	Текущий. Устный опрос.
19	Практическая работа. Эссе «Я и Интернет»		1	Практическая работа.	Стимулирование поведения и деятельности, направленных на соблюдение	Тематический. Индивидуальная работа.

					информационной безопасности.	
5.Мошеннические действия в Интернете. Киберпреступления (5 часов)						
20	Виды интернет – мошенничества. Опасность мобильной сети.	1		Лекция.	Развитие познавательной и творческой активности в безопасном использовании информационных и коммуникационных технологий.	Текущий. Работа в парах.
21	Техника безопасности при Регистрации на веб-сайтах.	1		Лекция.	Развитие компьютерной грамотности и информационной культуры личности в использовании информационных и коммуникационных технологий.	Текущий. Устный опрос.
22	Понятие компьютерное пиратство, плагиат.	1		Лекция.	Формирование умения соблюдать нормы информационной этики.	Текущий. Устный опрос.
23	Кибернаемники, кибердетективы.	1		Дискуссия.	Развитие сознательного и бережного отношения к вопросам собственной информационной безопасности	Текущий. Устный опрос.
24	Практическая работа. Круглый стол «Как не стать жертвой сетевых шуток и розыгрышей»		1	Практическая работа.	Развитие сознательного и бережного отношения к вопросам собственной информационной безопасности	Тематический. Групповая работа.
6.Агрессия в сети и ее виды (3 часа)						
25	Агрессия и агрессивность. Кибербуллинг.	1		Беседа.	Развитие познавательной и творческой активности в безопасном использовании информационных и	Текущий.

					коммуникационных технологий.	
26	Виды кибербуллинга.	1		Лекция.	Развитие сознательного и бережного отношения к вопросам собственной информационной безопасности	Текущий. Устный опрос.
27	Практическая работа. Рисунок «Моя киберагрессия»		1	Практическая работа.	Стимулирование поведения и деятельности, направленных на соблюдение информационной безопасности.	Тематический. Индивидуальная работа.
7.Троллинг в киберпространстве (3 часа)						
28, 29	Троллинг. Виды и типы троллинга.	2		Беседа.	Развитие сознательного и бережного отношения к вопросам собственной информационной безопасности	Текущий. Устный опрос.
30	Практическая работа. Информационный буклет «Не корми провокатора. Троллинг в интернете».		1	Практическая работа.	Развитие сознательного и бережного отношения к вопросам собственной информационной безопасности	Текущий. Индивидуальная работа.
8.Хейтинг: способы нейтрализации (3 часа)						
31	Хейтинг. Виды хейтеров.	1		Лекция.	Стимулирование поведения и деятельности, направленных на соблюдение информационной безопасности.	Текущий. Устный опрос.
32	Что делать, если вас хейтят?	1		Дискуссия.	Развитие сознательного и бережного отношения к вопросам собственной	Текущий. Устный опрос.

					информационной безопасности	
33	Практическая работа. Создание презентации «Хейтинг: способы нейтрализации?»		1	Практическая работа.	Развитие познавательной и творческой активности в безопасном использовании информационных и коммуникационных технологий.	Тематический. Индивидуальная работа.
34	Итоговое занятие.	1		Беседа.	Формирование умения соблюдать нормы информационной этики.	Итоговое. Коллективная работа.

