

РАССМОТРЕНО	СОГЛАСОВАНО	УТВЕРЖДАЮ
<p>на заседании МО Руководитель МО</p> <p>_____ /Таова Р.И./</p>	<p>Заместитель директора по ВР МБОУ «Гимназия № 4 г. Усть-Джегуты»</p> <p>_____ /Пазова М.И./</p>	<p>Директор МБОУ «Гимназия № 4 г. Усть-Джегуты»</p> <p>_____ /Байкулова А.М./</p>
<p>Протокол № 1 от 30.08.2023 года</p>	<p>30.08.2023 года</p>	<p>Приказ № 605 от 31.08.2023</p>



ПРОГРАММА ВНЕУРОЧНОЙ ДЕЯТЕЛЬНОСТИ

Название: «Кибербезопасность»

Класс: 7-9 классы

Срок реализации программы: 2023-2024 учебный год

Количество часов по учебному предмету: 1 час в неделю

Программу внеурочной деятельности составил: педагог
дополнительного образования Байчорова Аминат Азрет-Алиевна



Программа внеурочной деятельности «Кибербезопасность» для обучающихся 7-9 классов

Рабочая программа внеурочной деятельности курса «Кибербезопасность» для обучающихся 7-9 классов разработана в соответствии с локальными актами составлена на основе федерального государственного образовательного стандарта общего образования и на основании следующих нормативно-правовых документов:

1. Федеральный государственный образовательный стандарт основного общего образования (утвержден приказом Минобрнауки РФ от 17-12-2010 № 1897, с изменениями и дополнениями, в актуальной редакции).
2. Примерная основная образовательная программа основного общего образования (одобрена федеральным учебно-методическим объединением по общему образованию, протокол заседания от 08.04.2015 № 1/15).
3. Письмо Минобрнауки России от 14.12.2015 N 09-3564 "О внеурочной деятельности и реализации дополнительных общеобразовательных программ" (вместе с "Методическими рекомендациями по организации внеурочной деятельности и реализации дополнительных общеобразовательных программ").

Содержание и календарно-тематическое планирование рабочей программы внеурочной деятельности курса «Кибербезопасность» для обучающихся 8 классов составлено на основе учебного пособия «Информационная безопасность, или На расстоянии одного вируса. 7-9 классы: учеб. пособие для общеобразоват. организаций - М.: Просвещение, 2019 – 79 с. - (ФГОС. Внеурочная деятельность)». Данное пособие предназначено для организации внеурочной деятельности школьников 7-9 классов. Пособие знакомит школьников с правилами безопасного общения в сети Интернет, правилами защиты устройств и личной информации. В пособии содержатся разнообразные задания, выполнение которых не только способствует освоению материала курса, но и развивает у обучающихся коммуникативные навыки, умение работать в команде, умение критически анализировать возникающие ситуации и предложенные задачи, формирует навыки проектно-исследовательской деятельности учащихся.

Развитие современного информационного общества предполагает внедрение информационно-коммуникационных технологий во все сферы жизни человека: культура, образование, медицина, экономика и т.д. Современное общество очень активно использует разные виды ИКТ в своей практической деятельности, что соответствует положительной динамике развития общества в целом, но здесь появляется ряд новых проблем, связанных с безопасностью киберпространства, наличием кибератак, раскрытием персональных данных, утечки важной информации,

кибертерроризма. В проекте Концепции стратегии кибербезопасности Российской Федерации киберпространство определяется как «сфера деятельности в информационном пространстве, образованная совокупностью Интернета и других телекоммуникационных сетей и любых форм осуществляемой посредством их использования человеческой активности (личности, организации, государства)», а кибербезопасность – как «совокупность условий, при которых все составляющие киберпространства защищены от максимально возможного числа угроз и воздействий с нежелательными последствиями». В связи с этим большое значение приобретает проблема формирования культуры безопасного поведения в киберпространстве.

В соответствии со «Стратегией развития отрасли информационных технологий в Российской Федерации на 2014-2020 годы и на перспективу до 2025 года», утвержденной распоряжением Правительства Российской Федерации от 1 ноября 2013 г. № 2036-р, «Стратегией развития информационного общества в Российской Федерации», утвержденной Президентом Российской Федерации 7 февраля 2008 г. № Пр-212 и рядом других документов, Правительство Российской Федерации ставит перед собой следующие основные цели развития отрасли информационных технологий:

- обеспечение различных сфер экономики качественными информационными технологиями с целью повышения производительности труда;
- обеспечение высокого уровня информационной безопасности государства, индустрии и граждан.

Основными задачами по развитию отрасли информационных технологий России являются:

- развитие человеческого капитала, в том числе за счет развития профильного образования и популяризации профессий отрасли;
- повышение грамотности населения в области информационных технологий;
- обеспечение информационной безопасности;
- развитие широкополосного доступа в сеть "Интернет".

Учитывая выше указанные задачи Правительства РФ формирование культуры безопасного поведения в сети Интернет, социальных сообществах, «облачных» сервисах необходимо начинать при изучении учебной дисциплины «Информатика и ИКТ». Курс внеурочной деятельности «Кибербезопасность» направлен на решение поставленных задач и является продолжением непрерывного информационного образования в школе, возможностью дополнения учебной программы по информатике вопросами кибербезопасности.

Цель программы: создание условий для формирования у обучающихся знаний, умений и навыков, необходимых для организации безопасного поведения в сети Интернет и безопасности личного информационного пространства.

Задачи программы:

Образовательные:

1. Способствовать формированию знаний о безопасном поведении при работе с компьютерными программами, поиском информации в сети Интернет;
2. Формировать общие представления о существующих киберугрозах, кибератаках и правилах действий при встрече с ними в глобальной сети;
3. Формировать умения защитить себя и технические устройства при обнаружении ошибок и заражения вредоносными программами;
4. Формировать умения безопасной работы с информацией, анализировать и обобщать полученную информацию, критически относиться к информации и к выбору источника информации.

Развивающие:

1. Развивать компьютерную грамотность, информационную культуру личности в использовании информационных и коммуникационных технологий;
2. Соблюдать нормы информационной этики и права, этикета при работе в сети Интернет,
3. Развивать умение анализировать и систематизировать имеющуюся информацию;
4. 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. Формировать основы культуры умственного труда и взаимодействия с окружающими, ответственного отношения к вопросам безопасности жизнедеятельности;
4. Популяризировать профессии, связанные с информационными технологиями и безопасностью их применения.

Данная программа была разработана с учетом возрастных и психолого-педагогических особенностей учащихся среднего школьного возраста (7-9 класс). В этом возрасте происходит формирование технического и научного типа мышления, навыков исследовательской и проектной деятельности, самостоятельное осмысление межпредметных связей, анализ и сопоставление учебного материала с личным опытом. Содержание теоретического материала учебного курса тесно связано с личной значимостью и практической деятельностью обучающихся.

Программой предусмотрено использование современных учебных материалов, в число которых входят цифровые образовательные ресурсы: мультимедийные презентации, интерактивные обучающие уроки, видеоуроки, занимательные и развивающие игры, викторины, кроссворды по основным разделам курса внеурочной деятельности, разноуровневые тренировочные и проверочные материалы для организации фронтальной и индивидуальной работы, материально - техническая база мобильного класса. 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.

Для анализа результатов деятельности учащихся используются современные оценочные средства. В процессе реализации курса внеурочной деятельности «Кибербезопасность» выделено несколько форм контроля на понимание материала и умение применять знания на практике: тесты на образовательных платформах, рефлексия в ходе занятий, выполнение теоретических и практических упражнений, написание сообщений, проектов, пополнение портфолио по результатам конкурсов и олимпиадам по информационной безопасности. При этом используются следующие методы обучения: объяснение, учебная демонстрация, практические работы, консультации, анкетирование, чтение и анализ научно-популярных статей, посещение тематических онлайн-выставок, организация и проведение мастер-классов, онлайн-курсов. На учебном занятии обучающиеся заполняют рефлексивные листы, которые дают возможность учителю вносить коррективы в содержание учебного материала курса, а обучающемуся отслеживать успешность прохождения курса. На итоговом занятии обучающиеся и учитель подводят результаты по освоению всего курса в целом. В качестве зачётной итоговой работы может быть выставка буклетов, выступления обучающихся по актуальным вопросам информационной безопасности с собственными мультимедийными презентациями на ученических мероприятиях.

Данная программа в полной мере способствует активному развитию образовательной среды школы, оказывая влияние и создавая условия для формирования личности в социальном и пространственно-предметном окружении.

Описание места учебного курса в учебном плане

Рабочая программа внеурочной деятельности предназначена для учащихся 7-9 класса, рассчитана на 34 часов (1 часа в неделю).

Планируемые результаты освоения курса:

Рабочая программа обеспечивает формирование личностных, метапредметных и предметных результатов в соответствии с Федеральным Государственным Образовательным Стандартом.

Личностные результаты:

- формирование ответственного отношения к учению, готовности и способности обучающихся к саморазвитию и самообразованию на основе мотивации к обучению и познанию;
- формирование целостного мировоззрения, соответствующего современному уровню развития науки и общественной практики;
- развитие осознанного и ответственного отношения к собственным поступкам;
- формирование коммуникативной компетентности в процессе образовательной, учебно-исследовательской, творческой и других видов деятельности.

В сфере развития познавательных универсальных учебных действий приоритетное внимание уделяется:

- практическому освоению обучающимися основ проектно-исследовательской деятельности;
- развитию стратегий смыслового чтения и работе с информацией;
- практическому освоению методов познания, соответствующего им инструментария и понятийного аппарата, регулярному обращению в учебном процессе к использованию общеучебных умений, знаково-символических средств, широкого спектра логических действий и операций.

Метапредметные результаты:

- умение самостоятельно определять цели обучения, ставить и формулировать новые задачи в учебе и познавательной деятельности, развивать мотивы и интересы своей познавательной деятельности;
- умение соотносить свои действия с планируемыми результатами, осуществлять контроль своей деятельности в процессе достижения результата;
- навыки отбирать инструменты для оценивания своей деятельности, осуществлять самоконтроль своей деятельности в рамках предложенных условий и требований;

- умение наблюдать и анализировать собственную учебную и познавательную деятельность и деятельность других обучающихся в процессе взаимопроверки;
- умение определять понятия, создавать обобщения, устанавливать аналогии, классифицировать, самостоятельно выбирать основания и критерии для классификации, устанавливать причинно-следственные связи, строить логическое рассуждение, умозаключение;
- развитие мотивации к овладению культурой активного использования словарей и других поисковых систем;
- умение организовывать учебное сотрудничество и совместную деятельность с учителем и сверстниками; работать индивидуально и в группе;
- умение осознанно использовать речевые средства в соответствии с задачей коммуникации для выражения своих чувств, мыслей и потребностей для планирования и регуляции своей деятельности.

В рамках предметных результатов вопросы информационной безопасности обозначены как:

- формирование навыков и умений безопасного и целесообразного поведения при работе с компьютерными программами в Интернете, умения соблюдать нормы информационной этики и права;
- умение использовать средства информационных и коммуникационных технологий в решении когнитивных, коммуникативных и организационных задач с соблюдением требований эргономики, техники безопасности, гигиены, ресурсосбережения, правовых и этических норм, норм информационной безопасности;
- умение оценивать правильность выполнения учебной задачи, собственные возможности ее решения;
- формирование представлений о существующих киберугрозах и правилах действий при встрече с ними в глобальной сети;
- умение защитить себя и технические устройства при обнаружении ошибок и заражения вредоносными программами;

- понимание основ правовых аспектов использования компьютерных программ и работы в Интернете;
- формирование и развитие учащихся, проявляющих склонности и способности к информатике и ее изучению.

Виды деятельности: познавательная, проблемно-ценностное общение, практическая работа, проектная деятельность.

Содержание рабочей программы

Раздел 1. Общие сведения о безопасности ПК и Интернета

Как компьютер помогает науке и почему он нуждается в защите. Наука о защите компьютеров. Поиск информации в Интернете. Доступ к разрешенной информации - что это такое. Поиск в Интернете. Где Интернет хранит свои данные. Как сохранить в сети найденную информацию. Что такое облачные сервисы - безопасны ли они? Поиск документов в сети - все ли найденные данные правдивы и полезны? Как защитить себя от информационной перегрузки. Поиск информации в сети: к чему ведет переход по вредоносным ссылкам. Опасная информация в сети. Виды Интернет-общения. Общение в Интернете - переписка, форумы, социальные сети. Совместные игры в Интернете. Безопасно ли общение в Интернете? Когда появились компьютер и Интернет. Как вместе с Интернетом появились его болезни. Что такое дистанционное обучение. Есть ли у него минусы? Что такое компьютерная грамотность Интернет, телефон и космос. Польза и опасности мобильной связи. День системного администратора и день программиста - что это за профессии?

Основные понятия: кибербезопасность, Интернет, программное и аппаратное обеспечение, облачные сервисы, информационная перегрузка, дистанционное обучение, администратор, программист.

Формы работы: практикум, индивидуальная работа, проектная деятельность

Раздел 2. Техника безопасности и экология

Из чего сделан компьютер. Архитектура ЭВМ. Уход за компьютером. Гигиена при работе с компьютером. Как загрязняется компьютер. Техника безопасности при работе за компьютером. Режим проветривания. Временные интервалы работы за компьютером. Физическая нагрузка при работе с техникой. Перенапряжение. Усталость. Заболевания при нарушении временного режима работы за компьютером.

Компьютер и кровообращение. Воздействие электронных устройств на организм. Воздействие на зрение ЭЛТ, жидкокристаллических, светодиодных, монохромных мониторов. Как правильно сидеть за компьютером. Использование электронных устройств при неблагоприятных условиях. Вредит ли компьютер экологии (излучения, волны). Воздействие компьютера на зрение и другие органы. Польза и вред компьютерных игр. «Игровая» зависимость. Изменение сознания при «игровой» зависимости. Компьютер и недостаток движения. Компьютер и ЗОЖ. Физическое и психическое здоровье. Профилактика зрения. Виды зрительных упражнений. Что делать с компьютером в чрезвычайных ситуациях.

Основные понятия: вредный контент, техника безопасности, «игровая» зависимость, излучение, гигиена компьютера, психическое здоровье.

Формы работы: практикум, индивидуальная работа, проектная деятельность, уроки - «погружения», лекции.

Раздел 3. Проблемы Интернет-зависимости

Если слишком долго находиться в Интернете: что такое интернет-зависимость? Аддикция. Интернет-зависимость. Интернет как наркотик. Виртуальное общение. Виды виртуального общения. Кто создаёт способы и площадки виртуального общения. Социальные сети. История создания социальных сетей. Популяризация социальных сетей. Детские социальные сети. Безопасность личной информации. Какую информацию о себе следует выкладывать в сеть? Какая информация принадлежит вам? Не слишком ли много у вас друзей в социальной сети? Способы распространения негативной информации о Вас и Ваших родственниках. Взломы аккаунтов в социальных сетях. Последствия взломов. Виртуальная личность - что это такое? Зависимость от Интернет-общения в социальных сетях. Психическая зависимость. Нарушения психики. Агрессия. Негативное восприятие мира. Усталость. Нарушение сна. Замкнутость. Развлечения в Интернете. Виды развлечений. Игры: полезные и вредные. Признаки игровой зависимости. Профилактика игровой зависимости. Сетевые игры.

Основные понятия: социальная сеть, интернет-зависимость, сетевые игры, интернет-общение.

Формы работы: практикум, лекции, семинары, проектная деятельность.

Раздел 4. Методы обеспечения безопасности ПК и Интернета. Вирусы и антивирусы

Кто и зачем пишет вредоносные программы? Типы вредоносных программ. Воздействие вредоносных программ на работоспособность компьютера. Правильно ли работает компьютер? Признаки работы вирусов. Ищите в Интернете только то, что вам требуется. Методы безопасного поиска информации в сети Интернет. Как защититься от вредного контента. Что такое контент-фильтры. Поиск информации. Что такое поисковые серверы? Как с их помощью защитить себя от нежелательной информации. Родительский контроль. Какие программы для этого существуют. Детские браузеры. Виды детских браузеров. Детские сайты. Популярные браузеры и сайты для детей. Поиск информации. Антивирус. Принципы работы антивирусов. Классификация антивирусных программ. Платные, бесплатные антивирусные программы, демо-версии. Установка и функционирование антивирусных программ. Плюсы и минусы популярных антивирусов.

Основные понятия: компьютерный вирус, программы-боты, антивирусная программа (антивирус), родительский контроль, контент-фильтры, детские браузеры и сайты.

Формы работы: практикум, индивидуальная работа, проектная деятельность, уроки - «погружения»

Раздел 5. Мошеннические действия в Интернете. Киберпреступления

Поиск информации: если у вас требуют личную информацию при скачивании данных. Что такое личная информация? Данные о себе, родственниках – как и где посмотреть. Мошенничество. Виды киберпреступлений. Вредоносные атаки. Основные принципы воздействия на человека. Психология общения мошенника. Основные правила ведения разговора киберпреступника. Если вам сообщают о выигрыше в лотерею. Если вам предлагают установить новое приложение. Если вам предлагают бесплатные игры. Если вам предлагают что-то купить. Возможные последствия интернет-обмана. Способы предотвращения интернет-мошенничества. Профилактика безопасности против киберпреступлений.

Основные понятия: киберпреступление, интернет-мошенничество, пароль, логин, аккаунт, бесплатные игры.

Формы работы: практикум, деловая игра, проектная деятельность, лекции.

Раздел 6. Сетевой этикет. Психология и сеть

Что такое интернет-этикет? Сетевой этикет. Правила общения в сети Интернет. Компьютерная грамотность. Компьютерный словарный запас. Как вести себя «в гостях» у сетевых друзей. Психология участников интернет-общения. Кто «сидит» по ту сторону монитора. Разные типажи представителей социальных групп. Особенности общения в социальных группах. Помогает ли компьютер стать лучше? Общение в социальных сетях. Этикет в Интернете при работе с проектом в группе. Администратор, модератор – их деятельность и участие в общении виртуальных людей. Кто следит за общением виртуальных людей. Опасность интернет-общения. Урегулирование правовых споров. Федеральный закон «Об информации, информационных технологиях и о защите информации». Основные выдержки из Закона РФ.

Основные понятия: интернет-этикет, форум, администратор, модератор.

Формы работы: практикум, лекции, семинары.

Календарно-тематическое планирование

№	Дата занятия		Темы раздела, занятия	Самостоятельная деятельность учащихся	Кол-во часов	Примечание
	план	факт				
1.			Что такое кибербезопасность?	Групповая работа: создание мультимедийной презентации по теме «Основы кибербезопасности»	1	
2.			Доступ к разрешенной информации	Подготовка сообщения «Что такое доступ к разрешенной информации?» с использованием Интернет-словаря и справочника	1	
3.			Поиск документов в сети. Проверка правдивости информации	Индивидуальная работа по карточкам «Поиск информации в сети»	1	
4.			Виды компьютерных вирусов	Создание мультимедиа презентации «Компьютерные вирусы и их виды»	1	
5.			Уход за	Работа с поиском рефератов и сообщений в	1	

			компьютером. Гигиена при работе с компьютером	сети Интернет, составление памятки «Гигиена при работе за компьютером»		
6.			Воздействие электронных устройств на организм, воздействие на зрение	Подготовка сообщения «Вредные и опасные факторы при работе за компьютером»	1	
7.			Как правильно сидеть за компьютером	Составление памятки «Профилактика здоровья при работе за компьютером»	1	
8.			Использование электронных устройств при неблагоприятных условиях	Составление рабочего листа «Техника безопасности при неблагоприятных условиях»	1	
9.			Польза и вред компьютерных игр	Составление сравнительной таблицы «Польза и вред компьютерных игр»	1	
10.			Компьютер и здоровый образ жизни	Прохождение тестирования на образовательной платформе РЭШ	1	
11.			Интернет-зависимость. Интернет-как наркотик	Составление кластера «Причины появления Интернет-зависимости»	1	
12.			Виртуальное общение. Виды виртуального общения	Выполнение рисунка «Мой виртуальный друг»	1	
13.			Социальные сети	Написание эссе в текстовом документе на тему «Почему мне нравится «жить» в социальных сетях?»	1	
14.			Популяризация социальных сетей	Прохождение викторины «Что я знаю про социальные сети?»	1	
15.			Безопасность личной информации	Создание списка «Что нельзя сообщать о себе в сети Интернет» в текстовом документе	1	

16.			Способы распространения негативной информации	Подготовка мультимедийной презентации «Способы распространения негативной информации»	1	
17.			Взломы аккаунтов в социальных сетях	Подготовка сообщения	1	
18.			Виртуальная личность - что это такое?	Работа в команде с текстом веб-страницы: обсуждение и выявление главных признаков виртуальной личности	1	
19.			Зависимость от Интернет-общения в социальных сетях	Создание инструкции «Как вести себя в социальных сетях?»	1	
20.			Виды психических нарушений как следствие интернет-зависимости	Подготовка командной ролевой игры «Лечение болезни 21 века»	1	
21.			Признаки игровой зависимости	Групповая работа: создание анкеты для школьника «Есть ли у меня игровая зависимость?»	1	
22.			Кто и зачем пишет вредоносные программы?	Знакомство с курсом «Безопасность в Интернете» образовательной платформы stepic.org https://stepik.org/course/191/promo#toc	1	
23.			Признаки работы компьютерных вирусов	Изучение курса https://stepik.org/course/191/promo#toc	1	
24.			Методы безопасного поиска информации в сети Интернет	Изучение курса https://stepik.org/course/191/promo#toc	1	
25.			Родительский контроль	Написание эссе в текстовом документе на тему «Зачем нужен родительский контроль?»	1	
26.			Популярные браузеры и сайты для детей	Составление интерактивного кроссворда на образовательной платформе OnlineTestPad	1	
27.			Антивирусные программы.	Чтение и анализ научно-популярной статьи	1	

			Принципы работы антивирусов			
28.			Плюсы и минусы популярных антивирусов	Составление сравнительной таблицы по теме «Какой антивирус самый лучший?»	1	
29.			Что такое личная информация?	Чтение и анализ правовых статей	1	
30.			Мошенничество. Виды киберпреступлений	Групповая работа: создание мультимедиа презентации	1	
31.			Чем опасны онлайн- игры в Интернете	Командная работа: разработка теста- опросника «Чем опасны онлайн-игры в Интернете?»	1	
32.			Интернет- мошенничество и их виды	Групповая работа: Создание буклета	1	
33.			Сетевой этикет. Правила общения в сети Интернет	Разработка памятки «Правила общения в сети Интернет»	1	
34.			Опасность и угрозы общения в сети Интернет	Работа с индивидуальными карточками, в которых описываются разные ситуации	1	

Список использованной литературы:

1. Основы кибербезопасности: учебно-методическое пособие. 5—11 классы / С. Н. Вангородский. — М.: Дрофа, 2019. — 238, [1] с. — (Российский учебник).
2. Баранова Е.К., Бабаш А.В. Основы информационной безопасности: учебник / Е.К. Баранова, А.В. Бабаш. — М.: РИОР: ИНФРА-М, 2019. — 202 с. — (Среднее про - фессиональное образование)
3. Бирюков А.А. Информационная безопасность защита и нападение.: Издательство: ДМК-Пресс., 2018, 474 с.
4. Наместникова М.С. Информационная безопасность, или На расстоянии одного вируса. 7-9 классы: учеб.пособие для общеобразоват. организаций / М.С. Наместникова. – М.: Просвещение, 2019. – 79 с.: ил. – (Внеурочная деятельность).

5. Цветкова, М.С. Информационная безопасность. Кибербезопасность. 7–9 классы: учебное пособие /М.С. Цветкова, И.Ю. Хлобыстова. — 2-е изд., пересмотр. — М.: БИНОМ. Лаборатория знаний, 2020 — 64 с.: ил.
6. Шаньгин В.Ф. Информационная безопасность и защита информации. / Шаньгин В.Ф. – ДМК-Пресс, 2017 – 702 с.