Муниципальное автономное общеобразовательное учреждение
Школа № 56 им. Г.С. Овчинникова
городского округа город Уфа Республики Башкортостан

Рассмотрено
на заседании ШМО
учителей истории и
обществознания
Протокол № 1
от 24.08.2023г.
руководитель ШМО
_____А.В. Жидарева

Согласовано
ЗД по ВР
_____С.Е.Вервельская

25.08.2023

Утверждаю
Директор МАОУ Школа №56
им. Г.С. Овчинникова
_____Е.А. Ракитцкая
Приказ № 381 от 25.08.2023г.

Рабочая программа внеурочной деятельности
курса «Безопасность в сети "Интернет"»
направление общекультурное
5- 8 классы

Разработчик: заместитель директора по воспитательной работе Вервельская Снежана Евгеньевна

Уфа-2023

Программа курса внеурочной деятельности «Безопасность в сети «Интернет»»

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.

1 . Результаты освоения внеурочной деятельности

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 коммуникативных технологий;
2. Развиваются умения анализировать и систематизировать имеющуюся информацию;
3. Развиваются познавательная и творческая активность в безопасном использовании информационных и коммуникативных технологий.

Личностные:

1. Вырабатывается сознательное и бережное отношение к вопросам собственной информационной безопасности;
2. Формируются и развиваются нравственные, эстетические, патриотические качества личности;
3. Стимулируется поведение и деятельность, направленные на соблюдение информационной безопасности.

Способы определения планируемых результатов – педагогическое наблюдение, тесты, педагогический анализ результатов анкетирования, тестирования, опросов, участия в мероприятиях, защиты проектов, диагностику личностного роста и продвижения, педагогические отзывы и т.д.

2. Содержание курса с указанием форм организации и видов деятельности

5 классы (17 часов)

Тема № 1 Общие сведения о безопасности ПК и Интернета

Как устроен компьютер и интернет. Как работают мобильные устройства.угрозы для мобильных устройств. Защита персональных данных. Безопасный профиль в социальных сетях. Защита киберпространства как комплекс мероприятий, направленных на обеспечение информационной безопасности. Безопасный серфинг. Безопасные ресурсы для поиска.

Требования к знаниям и умениям: обучающиеся должны знать, как устроен компьютер и интернет, как работают мобильные устройства, что такое защита персональных данных; должны уметь защищать свои персональные данные составлять безопасные сети контактов, своевременно обнаружить проблемы сети, восстанавливать параметры систем.

Тематика практических работ:

Практическая работа № 1. Составить информационный буклет «Моя безопасная сеть».

Тема № 2. Техника безопасности и экология

Правила поведения в компьютерном классе.Компьютер и мобильные устройства в чрезвычайных ситуациях. Компьютер и зрение. Воздействие радиоволн на здоровье и окружающую среду.

Требования к знаниям и умениям: обучающиеся должны знать, правила поведения в компьютерном классе, как применяются компьютер и мобильное устройство в ЧС, какое влияние оказывает компьютер на зрение, какое воздействие оказывают радиоволны на здоровье человека и окружающую среду; должны уметь соблюдать требования ТБ при работе с компьютером, соблюдать гигиенические требования, проводить комплекс упражнений при работе за компьютером.

Тематика практических работ:

Практическая работа № 1. Создание буклета «Техника безопасности при работе с компьютером».

Тема № 3. Проблемы Интернет-зависимости

ЗОЖ и компьютер. Деструктивная информация в Интернете – как её избежать. Психологическое воздействие информации на человека. Управление личностью через Интернет. Интернет и компьютерная зависимость (аддикция). Критерии зависимости с точки зрения психологов. Как развивается зависимость. Типы интернет-зависимости.

Требования к знаниям и умениям: обучающиеся должны знать, что такое ЗОЖ, и как влияет компьютер на здоровье, какое психологическое воздействие оказывает информация на личностьчеловека, критерии зависимости, типы интернет-зависмости, как развивается зависимость; должны уметь распознавать и избегать деструктивную информацию в Интернете, уметь вовремя выявлять интернет-зависимость и сообщить специалистам.

Тематика практических работ:

Практическая работа № 1. Создание мультимедийной презентации «ПК и ЗОЖ. Организация рабочего места».

Тема № 4. Метод обеспечения безопасности ПК и Интернета. Вирусы и антивирусы.

Вирусы человека и компьютера, цели компьютерных вирусов. Типы вирусов. Отличие вирусов и закладок. Как распространяются вирусы. Что такое антивирусная защита. Как лечить компьютер. Антивирусные программы для ПК. Выявление неизвестных вирусов. Защита мобильных устройств. Безопасность при скачиваний 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 тп. Методы защиты фото и видеоматериалов от копирования в сети. Проверка подлинности в Интернете. Меры личной безопасности при сетевом общении. Настройка приватности в сетях. Предотвращение несанкционированного доступа к ПК.

Требования к знаниям и умениям: обучающиеся должны знать типы вирусов, что такое антивирусная защита, программы, как лечить компьютер, как защитить мобильные устройства, как защитить фото и видеоматериалы от скачиваний; должны уметь распознавать вирусы, пользоваться антивирусными защитными программами, соблюдать меры личной безопасности при сетевом общении..

Тематика практических работ:

Практическая работа № 1. «Установка антивирусной программы».

Практическая работа. № 2. Создание презентации на тему: «Троян-вымогатель в социальной сети «ВКонтакте» или наказание для особо любопытных».

Тема № 5. Мошеннические действия в Интернете. Киберпреступления.

Виды интернет-мошенничества. Фишинг. Мошеннические действия в сети. Предложения о разблокировании программ. Ложные антивирусы. Сбор «пожертвований» и благотворительность. «Легкий заработок» в Интернете. Пирамиды. Предложения по установке вредоносных приложений. Опасности мобильной связи. Азартные игры. Онлайн казино. Технология 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; должны уметь обезопасить себя при интернет-общении.

Тематика практических работ:

Практическая работа № 1. Доклад на тему: «Правила поведения в сети с мошенниками и злоумышленниками».

Тема № 6. Сетевой этикет. Психология и сеть.

Что такое сетевой этикет? Виды этикета. Различия этикета в разных странах. Как появился этикет и что это такое. Сетевой этикет. Этика дискуссий. Этикет и безопасность. Эмоции в сети, их выражение. Примеры этических нарушений. Безопасная работа в процессе сетевой коммуникации. Термины сетевого этикета. Психологическая обстановка в Интернете.

Требования к знаниям и умениям: обучающиеся должны знать сетевой этикет, этические и правовые нормы информационной деятельности человека, информационный этикет и право, информационную безопасность; должны уметь использовать этические и правовые нормы информационной деятельности человека, информационный этикет и право, информационную безопасность.

Тематика практических работ:

Практическая работа № 1. Выпуск видеоролика на тему: «Как не испортить себе настроение при общении в сети Интернет и не опуститься до уровня «веб-агрессора»

Тема № 7. Государственная политика в области кибербезопасности.

Собственности в Интернете. Авторское право. Интеллектуальная собственность. Платная и бесплатная информация. Защита прав потребителей при использовании услуг Интернета. 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.

Требования к знаниям и умениям: обучающиеся должны знать правовые основы защиты и информации, причиняющей вред здоровью и развитию, интеллектуальной собственности, уголовной ответственности за создание, использование и распространение вредоносных компьютерных программ, авторского право, охраны программ для ЭВМ и баз данных, лицензионных программ; должны уметь пользоваться правовыми основами защиты от информации, причиняющей вред здоровью и развитию, интеллектуальной собственности, уголовной ответственности за создание, использование и распространение вредоносных компьютерных программ, авторским правом, охраны программ для ЭВМ и баз данных, лицензионных программ

Тематика практических работ:

Практическая работа № 1. Буклет «Правовые основы для защита от спама».

Практическая работа № 2. Презентация «Как уберечь свою персональную информацию в Интернете, если вы общаетесь в социальных сетях».

9 классы (17 часов)

Тема № 1. Общие с ведения о безопасной работе в сети Интернет.

Борьба с использованием Интернета в террористических, сепаратистских и экстремистских целях. Интернет как оружие массового поражения. Социальные последствия безответственного поведения в Интернете. Безопасность платежных систем. Безопасность геоинформационных систем. Безопасность систем бронирования билетов. Безопасность при удаленном доступе к ресурчам компьютера. Хакерские атаки, их виды. Новые технологии и новые угрозы информационной безопасности. Рост числа угроз для мобильных устройств. Кибершпионаж.

Требования к знаниям и умениям: обучающиеся должны знать о возможном использовании Интернета в террористических, сепаратистских и экстремистских целях, о новых технологиях и новых угрозах информационной безопасности, о хакерских атаках; должны уметь ответственно и безопасно использовать возможности сети интернет для поиска. Хранения, использования информации и информационных услуг.

Тематика практических работ:

Практическая работа № 1. «Безопасные закупки в интернет- магазине»;

Практическая работа № 2. «создание буклета «Интернет, как оружие массового поражения»».

Практическая работа № 3. «Безопасность при удаленном доступе к ресурсам компьютера».

Тема № 2. Техника безопасности и экология

Персональный компьютер и ЗОЖ. Организация рабочего места.

Требования к знаниям и умениям: обучающиеся должны знать основы безопасности жизнедеятельности ЗОЖ, факторы, укрепляющие и разрушающие здоровье, вредные привычки и их профилактику, правила организации рабочего места; должны уметь правильно организовывать рабочее место, противостоять вредным привычкам.

Тематика практических работ:

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

Тема № 3. Проблемы Интернет-зависимости

Классификация интернет – зависимостей и их профилактика.

Требования к знаниям и умениям: обучающиеся должны знать классификацию интернет – зависимостей и способы профилактики; должны уметь классифицировать интернет – зависимости и проводить профилактику.

Тематика практических работ:

Практическая работа. Создание видеоролика на тему «Проблемы Интернет-зависимости».

Тема№ 4. Технические аспекты безопасного использования Интернета.

Аппаратная защита ПО и сети. Защита ПК на этапе загрузки. Параметры безопасности ПК. Обновления. Защита файловой системы. Файловые таблицы. Права доступа. Резервное копирование и восстановление данных. Восстановление ОС. Аппаратные и программные средства. Признаки заражения компьютерных программ. Где можно обнаружить подозрительные процессы. ОС и их возможности в борьбе с вирусами. Онлайн сервисы для безопасности пользователя в интернете. Защитное ПО. Антивирусные программы.межсетевые экраны. Брандмауэры. Как узнать местоположение компьютера по IP-адресу. Способы обеспечения безопасности веб-сайта. Коммерческое и бесплатное антивирусное ПО.

Требования к знаниям и умениям: обучающиеся должны знать аппаратную защиту ПО и сети, параметры безопасности ПК, защиту файловой системы, способы резервного копирования и восстановления данных, признаки заражения компьютерных программ, защитное ПО, антивирусные программы, межсетевые экраны, брандмауэры, способы определения местоположения компьютера по IP-адресу, способы обеспечения безопасности веб-сайта; должны уметь пользоваться программными средствами создания информационных объектов, организации личного информационного пространства, защиты информации, правилами подписки на антивирусные программы и их настройками на автоматическую проверку сообщений.

Тематика практических работ:

Практическая работа № 1. «Установка антивирусной программы»

Практическая работа № 2. «Создание буклета «Аппаратная защита ПО и сети»»

Практическая работа № 3. «Как узнать местоположение компьютера по IP-адресу.»

Практическая работа № 4. «Создание мультимедийной презентации «Разновидности вирусов. Шпионские программы. Шифровальщики. Хакерские утилиты. Сетевые атаки.»»

Тема № 5. Мошеннические действия в Интернете.

Техника безопасности при регистрации на веб-сайтах. ТБ на сайтах знакомств. Компьютерное пиратство. Плагиат. Кибернаемники и кибердетективы. Оценка ущерба от киберпреступлений.

Требования к знаниям и умениям: обучающиеся должны знать ТБ при регистрации на веб-сайтах, сайтах знакомств, понятия компьютерное пиратство,плагиат, кибернаемники и кибердетективы; должны уметь использовать правовые нормы, относящиеся к информации, правонарушениям в информационной сфере, меры их предотвращения, личную информацию, информационную безопасность, информационное право.

Тематика практических работ:

Практическая работа. «Подготовка электронного плаката «Безопасное использование сети Интернет»».

Тема № 6. Информационная этика.

Сетевой этикет. Значение сетевого этикета.

Требования к знаниям и умениям: обучающиеся должны знать сетевой этикет, этические и правовые нормы информационной деятельности человека, информационный этикет и право, информационную безопасность; должны уметь использовать этические и правовые нормы информационной деятельности человека, информационный этикет и право, информационную безопасность.

Тематика практических работ:

Практическая работа. «Выпуск видеоролика на тему «Сетевой этикет»».

Тема № 7. Информационное право и информационная безопасность в киберпространстве

Ответственность за киберпреступления. Конституционное право на поиск, получение и распространение информации. ФЗ от 29.12.2010 N 436-ФЗ (ред. От 28.07.2012) «о защите детей от информации, причиняющей вред их здоровью и развитию». Информационное законодательство РФ. Закон РФ «Об информации, информационных технологиях и о защите информации. «Уголовная ответственность за создание, использование и распространение вредоносных компьютерных программ». Правовая охрана программ для ЭВМ и БД. Коммерческое ПО. Бесплатное ПО, условно-бесплатное ПО. Правовые основы для защиты от спама. Правовые основы защиты интеллектуальной собственности. Авторское право. Правовая охрана программ для ЭВМ и баз данных. Лицензионное ПО. Виды лицензий. ПО с открытым кодом.

Требования к знаниям и умениям: обучающиеся должны знать правовые основы защиты от информации, причиняющей вред здоровью и развитию, интеллектуальной собственности, уголовной ответственности за создание, использование и распространение вредоносных компьютерных программ, авторского права, охраны программ для ЭВМ и баз данных, лицензионных программ; должны уметь пользоваться правовыми основами защиты от информации, причиняющей вред здоровью и развитию, интеллектуальной собственности, уголовной ответственности за создание, использование и распространение вредоносных компьютерных программ, авторским правом, охраны программ для ЭВМ и баз данных, лицензионных программ.

Тематика практических работ:

Практическая работа № 1. «Буклет «Правовые основы для защиты от спама»».

Практическая работа № 2. «Создание презентации «Правовая охрана программ для ЭВМ и БД. Коммерческое ПО. Бесплатное ПО»».

Тема № 8. Государственная политика в области кибербезопасности.

Информационная война. Информационное оружие. Защита киберпространства как одна из задач вооруженных сил. Какие органы власти отвечают за защиту киберпространства. Военная, государственная, коммерческая тайна. Защита сайтов государственных органов.

Требования к знаниям и умениям: обучающиеся должны знать основы защиты киберпространства, военной, государственной, коммерческой тайны; должны уметь ориентироваться в государственной политике в области кибербезопасности.

Тематика практических работ:

Практическая работа. «Создание презентации «Информационная война. Информационное воздействие»».

Формы подведения итогов: 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.

3.Тематическое планирование

5 классы

№ п/п	Тема	Количество часов	Количество аудиторных часов	Количество внеаудиторных часов
1	Общие сведения о безопасности ПК и Интернета	2	1	1
2	Техника безопасности и экология	3	2	1
3	Проблемы Интернет-зависимости	3	2	1
4	Метод обеспечения безопасности ПК и Интернета. Вирусы и антивирусы.	3	1	2
5	Мошеннические действия в Интернете. Киберпреступления.	2	1	1
6	Сетевой этикет. Психология и сеть.	2	1	1
7	Государственная политика в области кибербезопасности.	2	1	1
	Итого	17	9	8

9 классы

№ п/п	Тема	Количество часов	Количество аудиторных часов	Количество внеаудиторных часов
1	Общие сведения о безопасной работе в сети Интернет.	4	2	2
2	Проблемы Интернет-зависимости	1	1	
3	Технические аспекты безопасного использования Интернета.	5	2	3
4	Мошеннические действия в	3	2	1

	Интернете.			
5	Информационное право и информационная безопасность в киберпространстве	2	1	1
6	Государственная политика в области кибербезопасности.	2	1	1
	Итого	17	9	8