Муниципальное бюджетное общеобразовательное учреждение Школа №125
городского округа город Уфа Республики Башкортостан

Рассмотрено
на заседании ШМО
протокол №6
от «23» 03 2021 г.

Руководитель ШМО
Л.А.Сиргажина

Согласовано
заместитель
директора по ВР

М.Г.Старикова
«23» 03 2021 г.

Утверждаю
Директор МБОУ Школа№125

А.М.Абдразаков

Приказ №41
«01» 04 2021г

РАБОЧАЯ ПРОГРАММА
Курса внеурочной деятельности
«Безопасность в сети Интернет»
(основное общее образование
6-8 классы)

Составитель: Латыпова Д.Р.,
учитель информатики

класс 6-8

Рассмотрено на заседании
педагогического совета
протокол № 6
«23» 03 2021г.

1

1.Результат освоения учебного предмета, курса «Безопасность в сети интернет»

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.

Данная программа обеспечивает формирование следующих личностных, метапредметных и предметных результатов.
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.

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

2.Содержание учебного предмета, курса.

Тема № 1. (5 часов) - Общие сведения о безопасности ПК и Интернета

Основные вопросы: Как устроены компьютер и интернет. Как работают мобильные устройства. Угрозы для мобильных устройств. Защита персональных данных, почему она нужна. Категории персональных данных. Биометрические персональные данные. Безопасный профиль в социальных сетях. Составление сети контактов. Защита киберпространства как комплекс мероприятий, направленных на обеспечение информационной безопасности. Аспекты кибербезопасности Компьютерная и информационная безопасность, обнаружение проблем сети, восстановление параметров систем, средства защиты от несанкционированного доступа к данным, криптографическая защита информации. Основные угрозы безопасности информации: утечки, потеря целостности, нарушение работоспособности системы, незаконное тиражирование (воспроизведение). Безопасный серфинг. Безопасные ресурсы для поиска.
Тема № 2. (4 часа) - Техника безопасности и экология
Основные вопросы: Правила поведения в компьютерном классе. Техника безопасности при работе с компьютером. Компьютер и мобильные устройства в чрезвычайных ситуациях. Компьютер и зрение. Воздействие радиоволн на здоровье и окружающую среду (Wi-Fi, Bluetooth, GSM). Комплекс упражнений при работе за компьютером. Гигиена при работе с ПК
Тема № 3. (4 часа) - Проблемы Интернет-зависимости
Основные вопросы: ЗОЖ и компьютер. Деструктивная информация в Интернете - как ее избежать. Психологическое воздействие информации на человека. Управление личностью через сеть. Интернет и компьютерная зависимость (аддикция). Критерии зависимости с точки зрения психологов (приоритетность, изменения настроения, толерантность, симптом разрыва, конфликт, рецидив). Как развивается зависимость. Типы интернет - зависимости (пристрастие к работе с компьютером, к навигации и поиску информации, игромания и электронные покупки, зависимость от сетевого общения, сексуальные зависимости).
Тема № 4. (6 часов) - Методы обеспечения безопасности ПК и Интернета. Вирусы и антивирусы.
Основные вопросы: Вирусы человека и компьютера, цели компьютерных вирусов. Типы вирусов. Отличия вирусов и закладок. Как распространяются вирусы. Что такое антивирусная защита. Как лечить компьютер. Антивирусные программы для ПК: сканеры, ревизоры и др. Выявление неизвестных вирусов. Защита мобильных устройств. Безопасность при скачивании файлов. Защита программ и данных от несанкционированного копирования. Организационные, юридические, программные и программно-аппаратные меры защиты. Защита программ и данных с помощью паролей, программных и электронных ключей, серийных номеров, переноса в онлайн и т.п. Методы защиты фото и видеоматериалов от копирования в сети. Проверка подлинности (аутентификация) в Интернете. Меры личной безопасности при сетевом общении. Настройки приватности в социальных сетях. Предотвращение несанкционированного доступа к ПК. Пароли, биометрические методы защиты и аутентификация с помощью внешних носителей.
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.
Тема № 6. (5 часов) - Сетевой этикет. Психология и сеть
4. Основные вопросы: Что такое этикет. Виды этикета (личный, деловой, письменный, дискуссионный и пр.). Различия этикета в разных странах. Как появился этикет, что это такое. Сетевой этикет. Общие правила сетевого этикета. Этика дискуссий. Взаимное уважение при

интернет-общении. Этикет и безопасность. Эмоции в сети, их выражение. Примеры этических нарушений. Безопасная работа в сети в процессе сетевой коммуникации (чаты, форумы, конференции, скайп, социальные сети и пр.). Термины сетевого этикета: оверквотинг, флейм, флуд, оффтопик, смайлики и др. Психологическая обстановка в Интернете: грифинг, кибербуллинг, кибер-моббинг, троллинг, буллицид. Если вы стали жертвой компьютерной агрессии: службы помощи личное общение и общение в группе - чем они отличаются (чаты, форумы, службы мгновенных сообщений)
Тема №7. (5 часов) - Государственная политика в области кибербезопасности.
Основные вопросы: Собственность в Интернете. Авторское право. Интеллектуальная собственность. Платная и бесплатная информация. Защита прав потребителей при использовании услуг Интернет. Защита прав потребителей услуг провайдера. Как расследуются преступления в сети. Ответственность за интернет - мошенничество. Правовые акты в области информационных технологий и защиты киберпространства. Доктрина информационной безопасности.
Повторение и обобщение пройденных тем – 1 час

Формы и методы реализации внеурочной деятельности

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; закупки в интернет магазине; квесты; создание буклетов и мультимедийных презентаций.

Формами подведения итогов реализации дополнительной общеобразовательной программы «Безопасность в сети Интернет» могут быть 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.

В ходе реализации программы возможно использование различных **методов и приёмов** организации занятий:
по источнику получения информации: практический (опыты, упражнения);
наглядный (иллюстрация, демонстрация, наблюдения обучающихся); словесный (объяснение, разъяснение, рассказ, беседа, инструктаж, лекция, дискуссия, диспут);
работа с книгой (чтение, изучение, реферирование, цитирование, беглый просмотр, конспектирование);
идеометод (просмотр, обучение, упражнение, контроль);
по характеру дидактической цели:
приобретение знаний; формирование умений и навыков;
применение знаний; формирование творческой деятельности; закрепление и контроль знаний, умений, навыков;
по характеру познавательной деятельности:
поисковые; объяснительно-иллюстративные; репродуктивные; проблемного изложения;
эвристические (частично-поисковые); исследовательские;
по соответствию методов обучения логике общественно-исторического познания:
организация наблюдения, накопление эмпирического материала; обобщение теоретической обработки фактических данных;
практическая проверка правильности выводов и обобщений, выявление истины, соответствия содержания и формы, явления и сущности;
по соответствию методов обучения специфике изучаемого материала и форм мышления:

научного познания реальной действительности;
освоения искусства;
практического применения знаний.

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

Тематическое планирование с указанием количества часов на освоение каждой темы в 6А классе.

№ урока	Тема урока	Количество часов	Примерная дата проведения урока	Фактическая дата проведения урока
Тема 1. Общие сведения о безопасности ПК и Интернета – 5 часов				
1	Как устроены компьютер и Интернет. Как работают мобильные устройства. Угрозы для мобильных устройств	1	02.09	
2	Защита персональных данных, почему она нужна. Категории персональных данных. Биометрические персональные данные	1	09.09	
3	Безопасный профиль в социальных сетях. Составление сети контактов.	1	16.09	
4	Компьютерная и информационная безопасность, обнаружение проблем сети, восстановление параметров систем, средства защиты от несанкционированного доступа к данным, криптографическая защита информации	1	23.09	
5	Основные угрозы безопасности информации: утечки, потеря целостности, нарушение работоспособности системы, незаконное тиражирование. Безопасные ресурсы для поиска	1	30.09	
Тема 2. Техника безопасности и экология – 4 часов				
6	Правила поведения в компьютерном классе. Техника безопасности при работе с компьютером	1	07.10	
7	Компьютер и мобильные устройства в чрезвычайных ситуациях.	1	14.10	
8	Компьютер и зрение. Воздействие радиоволн на здоровье и окружающую среду (Wi-Fi,Bluetooth, GSM)	1	21.10	
9	Комплекс упражнений при работе за компьютером. Гигиена при работе с ПК	1	11.11	
Тема 3. Проблемы Интернет-зависимости – 4 часов				
10	ЗОЖ и компьютер.	1	18.11	
11	Деструктивная информация в Интернете – как ее избежать. Психологическое	1	25.11	

	воздействие информации на человека. Управление личностью через сеть			
12	Интернет и компьютерная зависимость (аддикция). Как развивается зависимость	1	02.12	
13	Типы интернет-зависимости (пристрастие к работе с компьютером, к навигации и поиску информации, игромания и электронные покупки, зависимость от сетевого общения и т.д.)	1	09.12	
Тема 4. Методы обеспечения безопасности ПК и Интернета. Вирусы и антивирусы – 6 часов				
14	Вирусы человека и компьютера, цели компьютерных вирусов. Типы вирусов	1	16.12	
15	Как распространяются вирусы. Что такое антивирусная защита. Как лечить компьютер. Антивирусные программы для ПК	1	23.12	
16	Защита мобильных устройств. Безопасность при скачивании файлов	1	06.01	
17	Защита программ и данных от несанкционированного копирования	1	13.01	
18	Проверка подлинности (аутентификация) в Интернете. Меры личной безопасности при сетевом общении	1	20.01	
19	Предотвращение несанкционированного доступа к ПК. Пароли, биометрические методы защиты и аутентификация с помощью внешних носителей	1	27.01	
Тема 5. Мошеннические действия в Интернете. Киберпреступления – 5 часов				
20	Виды интернет-мошенничества	1	03.02.	
21	Опасности мобильной связи	1	10.02.	
22	Азартные игры. Он-лайн казино. Букмекерские конторы	1	17.02	
23	Технологии манипулирования в Интернете	1	02.03	
24	Техника безопасности при интернет-общении	1	09.03	
Тема 6. Сетевой этикет. Психология и сеть - 5 часов				
25	Что такое этикет. Виды и различия в разных странах.	1	16.03	
26	Сетевой этикет	1	23.03	
27	Эмоции в сети, их выражение. Примеры этических нарушений	1	30.03	
28	Психологическая обстановка в Интернете: грифинг, кибербуллинг, кибер-моббинг, троллинг, буллицид.	1	06.04	
29	Если вы стали жертвой компьютерной агрессии	1	13.04	
Тема 7. Государственная политика в области кибербезопасности – 5 часов				
30	Собственность в Интернете. Авторское	1	20.04	

	право и интеллектуальная собственность			
31	Платная и бесплатная информация	1	27.04	
32	Как расследуются преступления в сети. Ответственность за интернет-мошенничество	1	04.05	
33	Правовые акты в области информационных технологий и защиты киберпространства	1	11.05	
34	Доктрина информационной безопасности	1	18.05	
35	Повторение и обобщение пройденных тем	1	25.05	

Тематическое планирование с указанием количества часов на освоение каждой темы в 7 классе.

№ урока	Тема урока	Количество часов	Примерная дата проведения урока	Фактическая дата проведения урока
Тема 1. Общие сведения о безопасности ПК и Интернета – 5 часов				
1	Как устроены компьютер и Интернет. Как работают мобильные устройства. Угрозы для мобильных устройств	1	02.09	
2	Защита персональных данных, почему она нужна. Категории персональных данных. Биометрические персональные данные	1	09.09	
3	Безопасный профиль в социальных сетях. Составление сети контактов.	1	16.09	
4	Компьютерная и информационная безопасность, обнаружение проблем сети, восстановление параметров систем, средства защиты от несанкционированного доступа к данным, криптографическая защита информации	1	23.09	
5	Основные угрозы безопасности информации: утечки, потеря целостности, нарушение работоспособности системы, незаконное тиражирование. Безопасные ресурсы для поиска	1	30.09	
Тема 2. Техника безопасности и экология – 4 часов				
6	Правила поведения в компьютерном классе. Техника безопасности при работе с компьютером	1	07.10	
7	Компьютер и мобильные устройства в чрезвычайных ситуациях.	1	14.10	

8	Компьютер и зрение. Воздействие радиоволн на здоровье и окружающую среду (Wi-Fi,Bluetooth, GSM)	1	21.10	
9	Комплекс упражнений при работе за компьютером. Гигиена при работе с ПК	1	11.11	
Тема 3. Проблемы Интернет-зависимости – 4 часов				
10	ЗОЖ и компьютер.	1	18.11	
11	Деструктивная информация в Интернете – как ее избежать. Психологическое воздействие информации на человека. Управление личностью через сеть	1	25.11	
12	Интернет и компьютерная зависимость (аддикция). Как развивается зависимость	1	02.12	
13	Типы интернет-зависимости (пристрастие к работе с компьютером, к навигации и поиску информации, игромания и электронные покупки, зависимость от сетевого общения и т.д.)	1	09.12	
Тема 4. Методы обеспечения безопасности ПК и Интернета. Вирусы и антивирусы – 6 часов				
14	Вирусы человека и компьютера, цели компьютерных вирусов. Типы вирусов	1	16.12	
15	Как распространяются вирусы. Что такое антивирусная защита. Как лечить компьютер. Антивирусные программы для ПК	1	23.12	
16	Защита мобильных устройств. Безопасность при скачивании файлов	1	06.01	
17	Защита программ и данных от несанкционированного копирования	1	13.01	
18	Проверка подлинности (аутентификация) в Интернете. Меры личной безопасности при сетевом общении	1	20.01	
19	Предотвращение несанкционированного доступа к ПК. Пароли, биометрические методы защиты и аутентификация с помощью внешних носителей	1	27.01	
Тема 5. Мошеннические действия в Интернете. Киберпреступления – 5 часов				
20	Виды интернет-мошенничества	1	03.02.	
21	Опасности мобильной связи	1	10.02.	
22	Азартные игры. Он-лайн казино. Букмекерские конторы	1	17.02	
23	Технологии манипулирования в Интернете	1	02.03	
24	Техника безопасности при интернет-общении	1	09.03	
Тема 6. Сетевой этикет. Психология и сеть - 5 часов				
25	Что такое этикет. Виды и различия в разных странах.	1	16.03	
26	Сетевой этикет	1	23.03	

27	Эмоции в сети, их выражение. Примеры этических нарушений	1	30.03	
28	Психологическая обстановка в Интернете: грифинг, кибербуллинг, кибер-моббинг, троллинг, буллицид.	1	06.04	
29	Если вы стали жертвой компьютерной агрессии	1	13.04	
Тема 7. Государственная политика в области кибербезопасности – 5 часов				
30	Собственность в Интернете. Авторское право и интеллектуальная собственность	1	20.04	
31	Платная и бесплатная информация	1	27.04	
32	Как расследуются преступления в сети. Ответственность за интернет-мошенничество	1	04.05	
33	Правовые акты в области информационных технологий и защиты киберпространства	1	11.05	
34	Доктрина информационной безопасности	1	18.05	
35	Повторение и обобщение пройденных тем	1	25.05	

Тематическое планирование с указанием количества часов на освоение каждой темы 8 класс

№ урока	Тема урока	Количество часов	Примерная дата проведения урока	Фактическая дата проведения урока
Тема 1. Общие сведения о безопасности ПК и Интернета – 5 часов				
1	Как устроены компьютер и Интернет. Как работают мобильные устройства. Угрозы для мобильных устройств	1	02.09	
2	Защита персональных данных, почему она нужна. Категории персональных данных. Биометрические персональные данные	1	09.09	
3	Безопасный профиль в социальных сетях. Составление сети контактов.	1	16.09	
4	Компьютерная и информационная безопасность, обнаружение проблем сети, восстановление параметров систем, средства защиты от несанкционированного доступа к данным, криптографическая защита информации	1	23.09	
5	Основные угрозы безопасности информации: утечки, потеря целостности, нарушение работоспособности системы, незаконное тиражирование. Безопасные ресурсы для	1	30.09	

	поиска			
Тема 2. Техника безопасности и экология – 4 часов				
6	Правила поведения в компьютерном классе. Техника безопасности при работе с компьютером	1	07.10	
7	Компьютер и мобильные устройства в чрезвычайных ситуациях.	1	14.10	
8	Компьютер и зрение. Воздействие радиоволн на здоровье и окружающую среду (Wi-Fi,Bluetooth, GSM)	1	21.10	
9	Комплекс упражнений при работе за компьютером. Гигиена при работе с ПК	1	11.11	
Тема 3. Проблемы Интернет-зависимости – 4 часов				
10	ЗОЖ и компьютер.	1	18.11	
11	Деструктивная информация в Интернете – как ее избежать. Психологическое воздействие информации на человека. Управление личностью через сеть	1	25.11	
12	Интернет и компьютерная зависимость (аддикция). Как развивается зависимость	1	02.12	
13	Типы интернет-зависимости (пристрастие к работе с компьютером, к навигации и поиску информации, игромания и электронные покупки, зависимость от сетевого общения и т.д.)	1	09.12	
Тема 4. Методы обеспечения безопасности ПК и Интернета. Вирусы и антивирусы – 6 часов				
14	Вирусы человека и компьютера, цели компьютерных вирусов. Типы вирусов	1	16.12	
15	Как распространяются вирусы. Что такое антивирусная защита. Как лечить компьютер. Антивирусные программы для ПК	1	23.12	
16	Защита мобильных устройств. Безопасность при скачивании файлов	1	06.01	
17	Защита программ и данных от несанкционированного копирования	1	13.01	
18	Проверка подлинности (аутентификация) в Интернете. Меры личной безопасности при сетевом общении	1	20.01	
19	Предотвращение несанкционированного доступа к ПК. Пароли, биометрические методы защиты и аутентификация с помощью внешних носителей	1	27.01	
Тема 5. Мошеннические действия в Интернете. Киберпреступления – 5 часов				
20	Виды интернет-мошенничества	1	03.02.	
21	Опасности мобильной связи	1	10.02.	
22	Азартные игры. Он-лайн казино. Букмекерские конторы	1	17.02	
23	Технологии манипулирования в	1	02.03	

	Интернете			
24	Техника безопасности при интернет-общении	1	09.03	
Тема 6. Сетевой этикет. Психология и сеть - 5 часов				
25	Что такое этикет. Виды и различия в разных странах.	1	16.03	
26	Сетевой этикет	1	23.03	
27	Эмоции в сети, их выражение. Примеры этических нарушений	1	30.03	
28	Психологическая обстановка в Интернете: грифинг, кибербуллинг, кибер-моббинг, троллинг, буллицид.	1	06.04	
29	Если вы стали жертвой компьютерной агрессии	1	13.04	
Тема 7. Государственная политика в области кибербезопасности – 5 часов				
30	Собственность в Интернете. Авторское право и интеллектуальная собственность	1	20.04	
31	Платная и бесплатная информация	1	27.04	
32	Как расследуются преступления в сети. Ответственность за интернет-мошенничество	1	04.05	
33	Правовые акты в области информационных технологий и защиты киберпространства	1	11.05	
34	Доктрина информационной безопасности	1	18.05	
35	Повторение и обобщение пройденных тем	1	25.05	