МИНИСТЕРСТВО ПРОСВЕЩЕНИЯ РОССИЙСКОЙ ФЕДЕРАЦИИ

Министерство образования Красноярского края

Отдел образования администрации Уярского района

МБОУ "Толстихинская СОШ"

РАССМОТРЕНО

На МО классных руководителей

Руководитель ШМО

_____

Беленко И.В.

Протокол № 1
от «28» 09 2024 г.

УТВЕРЖДЕНО

Директор школы

_____

Наконечная Н.Ф.

Приказ №227
от «28» 09 2024 г.

РАБОЧАЯ ПРОГРАММА

внеурочной деятельности

«Основы кибербезопасности»

Для 7 класса.

С. Толстихино 2024 год.

Рабочая программа

внеурочной деятельности

Основы кибербезопасности для учащихся 7 класса

I. Пояснительная записка

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.

Развитие информационного общества предполагает внедрение информационных технологий во все сферы жизни, но это означает и появление новых угроз безопасности – от утечек информации до 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 «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 в числе многих других задач выделяются:

- обеспечение различных сфер экономики качественными информационными технологиями;
- обеспечение высокого уровня информационной безопасности государства, индустрии и граждан.

Безопасность в информационном обществе является одним из основных направлений фундаментальных исследований в области информационных технологий.

Компьютерные технологии применяются при изучении практически всех школьных дисциплин уже с младших классов. Киберугрозы существуют везде, где применяются информационные технологии.

Государство считает необходимым расширение объема преподавания информационных технологий в общеобразовательных организациях. В качестве одной из организационных мер в обеспечении кибербезопасности определена разработка и внедрение в учебный процесс образовательных организаций разного уровня курса по информационной безопасности, включающего модули по обеспечению кибербезопасности, либо дополнение имеющихся курсов упомянутыми модулями. Школьная программа должна соответствовать этим целям, поэтому представляется актуальным реализация программы внеурочной деятельности «Основы кибербезопасности».

Задача курса «Основы кибербезопасности» - совершенствование школьного образования и подготовки в сфере информационных технологий, а также популяризация профессий, связанных с информационными технологиями. Цель изучения «Основ кибербезопасности» - дать общие представления о безопасности в информационном обществе и на этой основе сформировать понимание технологий информационной безопасности и умения применять правила кибербезопасности во всех сферах деятельности.

Воспитательная цель курса – формирование на качественно новом уровне культуры умственного труда и взаимодействия с окружающими, ответственного отношения к вопросам безопасности жизнедеятельности.

Цель программы – создание условий для формирования у учащихся цифровой культуры личности с необходимыми навыками и присущими ценностями, взглядами, ориентациями, установками, мотивами деятельности и поведения для обеспечения безопасной и развивающей жизнедеятельности учащегося в сети «Интернет».

Для достижения поставленной цели решаются следующие задачи:

- Формирование у учащихся цифровой и информационной культуры;
- Воспитание у учащихся нравственности и культуры взаимоотношения с людьми на основе общечеловеческих ценностей в сети «Интернет»;
- Утверждение в сознании и чувствах учащихся правильных моделей поведения, ценностей, взглядов и убеждений для успешной жизнедеятельности учащегося в сети «Интернет»;
- Углубление знаний учебных дисциплин «Информатика», «ОБЖ» и «Обществознание» в процессе обучения в рамках программы;
- Интеллектуальное развитие учащихся, формирование творческих и прикладных качеств мышления;
- Развитие интереса к различным сферам информационных технологий;
- Совершенствование навыков самообразования, всестороннего развития и социализации;
- Обучение поиску и отбору информации, её интерпретации и применимости;
- Развитие логического мышления, умений обобщения и конкретизации, анализа и синтеза;
- Воспитание умения трудиться, самостоятельности, ответственности и творческого отношения к учёбе;

Обучающие:

- Сформировать систему знаний в сфере обществознания, информационных технологий и основ безопасности жизнедеятельности;
- Обучить элементам системного мышления использовать инструменты активизации мышления;
- Отработка навыков и умений для безопасного и полезного использования информационных технологий: сравнение информации, критический анализ, выделение главных мыслей и грамотное изложение, а также восприятия и усвоения информации из сети «Интернет».

Развивающие:

- Развить интеллектуальные и социальные способности обучающихся;
- Развить навыки сетевого общения и коммуникации в сети «Интернет», поиска и работы с информацией, обеспечения безопасности цифровых устройств и аккаунтов и осуществления сетевых покупок;
- Развить деловые и гражданские качества, такие как самостоятельность, ответственность, активность и аккуратность;
- Сформировать потребности в самопознании и саморазвитии.

Воспитательные:

- Воспитать культуру общения и поведения в сетевом пространстве;
- Воспитать целеустремлённость личности;
- Воспитать толерантную и культурную личность;
- Воспитать правильный образ гражданина.

II. Общая характеристика курса

Курс «Основы кибербезопасности» структурирован по модульному принципу. Он включает в себя 7 модулей:

- Общие сведения о безопасности ПК и Интернета
- Техника безопасности и экология
- Проблемы Интернет-зависимости
- Методы обеспечения безопасности ПК и Интернета. Вирусы и антивирусы
- Мошеннические действия в Интернете. Киберпреступления
- Сетевой этикет. Психология и сеть
- Правовые аспекты защиты киберпространства

III. Описание места учебного предмета в учебном плане.

Данный курс реализуется в рамках социального направления внеурочной деятельности и рассчитан на 1 час в неделю (34 часа).

IV. Содержание учебного предмета

7 класс

Модуль 1. Общие сведения о безопасности ПК и Интернета (5 часов).

Как работают мобильные устройства. Угрозы для мобильных устройств.

Распространение вредоносных файлов через приложения для смартфонов и планшетов (скачивание фотографий, музыки, игр).

Виды защиты киберпространства (что такое несанкционированный доступ, разрушение и утрата информации, искажение информации).

Кто обеспечивает защиту киберпространства.

Что такое геоинформационные системы (ГИС). Глобальные информационные Сети по стихийным бедствиям.

Модуль 2. Техника безопасности и экология (5 часов).

Компьютер и мобильные устройства в чрезвычайных ситуациях. Дополнения к ДТП. Компьютер и мобильные (сотовые) устройства в правилах безопасности.

Компьютеры и мобильные устройства в экстремальных условиях.

Везде ли есть Интернет. ТБ при работе с мобильными устройствами.

Первая помощь при проблемах в интернете (службы помощи).

Воздействие радиоволн на здоровье и окружающую среду (Wi-Fi, Bluetooth, GSM).

Модуль 3. Проблемы Интернет-зависимости (2 часа).

Виды Интернет-зависимости.

Компьютер и зрение.

Модуль 4. Методы обеспечения безопасности ПК и Интернета. Вирусы и антивирусы (8 часов).

Вирусы и антивирусы.

Как распространяются вирусы.

Источники и причины заражения.

Скорая компьютерная помощь. Признаки заражения компьютера.

Что такое антивирусная защита. Как лечить компьютер.

Защита мобильных устройств.

Как защитить данные от потерь. Копирование и восстановление. Всегда ли можно спасти свои данные.

Защита файлов. Что такое право доступа.

Защита детей в социальных сетях. ПО для родителей. Ограничение времени нахождения в сети.

Модуль 5. Мошеннические действия в Интернете. Киберпреступления (2 часа).

Опасности мобильной связи. Предложения по установке вредоносных приложений. Мошеннические СМС.

Прослушивание разговоров. Определение местоположения телефона.

Модуль 6. Сетевой этикет. Психология и сеть (10 часов).

Что такое личные данные. Все, что выложено в Интернет, может стать известно всем.

«Лишняя информация» о себе и других в Интернете. Какая информация принадлежит вам.

Анонимность в сети.

Что такое этикет. Виды этикета (личный, деловой, письменный, дискуссионный и пр.). Различия этикета в разных странах.

Как появился нетикет, что это такое. Общие правила сетевого этикета.

Личное общение и общение в группе – чем они отличаются (чаты, форумы, службы мгновенных сообщений).

Этика дискуссий. Взаимное уважение при интернет-общении.

Этикет и безопасность. Эмоции в сети, их выражение.

Реальная и виртуальная личность, реальные встречи с виртуальными знакомыми и их опасность, угрозы и оскорбления – чем это может закончиться.

Если вы стали жертвой компьютерной агрессии: службы помощи.

Модуль 7. Правовые аспекты защиты киберпространства (2 часа).

Собственность в Интернете. Авторское право. Интеллектуальная собственность. Платная и бесплатная информация.

Обобщение материала курса. Игра-квест «Знатоки кибербезопасности».

V. Планируемые результаты изучения курса

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.

VI. Тематическое планирование

№ п/п	Наименование модулей	Кол-во часов		
		7 класс	8 класс	9 класс
1	Общие сведения о безопасности ПК и Интернета	5	5	11
2	Техника безопасности и экология.	5	2	3
3	Проблемы Интернет-зависимости	2	3	2
4	Методы обеспечения безопасности ПК и Интернета. Вирусы и антивирусы	8	16	7
5	Мошеннические действия в Интернете. Киберпреступления	2	4	7
6	Сетевой этикет. Психология и сеть	10	1	1
7	Правовые аспекты защиты киберпространства	2	3	3
	Всего часов:	**34**	**34**	**34**

VII. Учебно-методическое и материально-технического обеспечения образовательного процесса

Методические материалы
Тонких И.М., Комаров М.М., Ледовской В.И., Михайлов А.В. Основы кибербезопасности, Москва, 2016
Портал Международного квеста по цифровой грамотности www.Сетевичок.рф
https://toipkro.ru/content/files/documents/podrazdeleniya/ordo/ciber%20bezopasnost.pdf

Экранно-звуковые пособия
Видеофильмы по основным разделам курса
Презентации по тематике курса

Технические средства обучения
Ноутбук
Телевизор.
Мультимедиапроектор.
Экран навесной.
Средства телекоммуникации (электронная почта, выход в Интернет).

Учебно-практическое оборудование
Аудиторная доска с магнитной поверхностью

Календарно-тематическое планирование 7 класс (34 часа)

№ урока	Дата	Тема	Кол-во часов
		Общие сведения о безопасности ПК и Интернета	**5**
1		Как работают мобильные устройства. Угрозы для мобильных устройств.	
2		Распространение вредоносных файлов через приложения для смартфонов и планшетов (скачивание фотографий, музыки, игр).	
3		Виды защиты киберпространства (что такое несанкционированный доступ, разрушение и утрата информации, искажение информации).	
4		Кто обеспечивает защиту киберпространства.	
5		Что такое геоинформационные системы (ГИС). Глобальные информационные Сети по стихийным бедствиям.	
		Техника безопасности и экология.	**5**
6		Компьютер и мобильные устройства в чрезвычайных ситуациях. Дополнения к ДТП. Компьютер и мобильные (сотовые) устройства в правилах безопасности.	
7		Компьютеры и мобильные устройства в экстремальных условиях.	
8		Везде ли есть Интернет. ТБ при работе с мобильными устройствами.	
9		Первая помощь при проблемах в интернете (службы помощи).	
10		Воздействие радиоволн на здоровье и окружающую среду (Wi-Fi, Bluetooth, GSM).	
		Проблемы Интернет-зависимости.	**2**
11		Виды Интернет-зависимости.	
12		Компьютер и зрение.	
		Методы обеспечения безопасности ПК и Интернета. Вирусы и антивирусы.	**8**
13		Как распространяются вирусы.	
14		Источники и причины заражения.	
15		Скорая компьютерная помощь. Признаки заражения компьютера.	
16		Что такое антивирусная защита. Как лечить компьютер.	
17		Защита мобильных устройств.	
18		Как защитить данные от потерь. Копирование и восстановление. Всегда ли можно спасти свои данные.	
19		Защита файлов. Что такое право доступа.	
20		Защита детей в социальных сетях. ПО для родителей. Ограничение времени нахождения в сети.	
		Мошеннические действия в Интернете. Киберпреступления.	**2**
21		Опасности мобильной связи. Предложения по установке вредоносных приложений. Мошеннические СМС.	
22		Прослушивание разговоров. Определение местоположения телефона.	
		Сетевой этикет. Психология и сеть.	**10**
23		Что такое личные данные. Все, что выложено в Интернет, может стать известно всем.	
24		«Лишняя информация» о себе и других в Интернете. Какая информация принадлежит вам.	
25		Анонимность в сети.	
26		Что такое этикет. Виды этикета (личный, деловой, письменный,	

		дискуссионный и пр.). Различия этикета в разных странах.	
27		Как появился нетикет, что это такое. Общие правила сетевого этикета.	
28		Личное общение и общение в группе – чем они отличаются (чаты, форумы, службы мгновенных сообщений).	
29		Этика дискуссий. Взаимное уважение при интернет-общении.	
30		Этикет и безопасность. Эмоции в сети, их выражение.	
31		Реальная и виртуальная личность, реальные встречи с виртуальными знакомыми и их опасность, угрозы и оскорбления – чем это может закончиться.	
32		Если вы стали жертвой компьютерной агрессии: службы помощи.	
		Правовые аспекты защиты киберпространства.	**2**
33		Собственность в Интернете. Авторское право. Интеллектуальная собственность. Платная и бесплатная информация.	
34		Обобщение материала курса. Игра-квест «Знатоки кибербезопасности».	