МКУ «Управление образования Чернянского района»
Белгородской области

Рассмотрена на заседании МЭС
Протокол №4 от 22 декабря 2020 года

Утверждаю:
Начальник МКУ «Управление образования Чернянского района»
_____ М.Г. Верченко

ДОПОЛНИТЕЛЬНАЯ ОБЩЕОБРАЗОВАТЕЛЬНАЯ ПРОГРАММА
«Безопасность в сети Интернет»

(для обучающихся 1-11 классов с учетом возрастных категорий,
срок реализации 3 месяцев)
Направленность: техническая
Уровень программы: базовый

Составитель программы: Долгушин Александр Владимирович начальник отдела информационно - технологического сопровождения УО

2021 год

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. Программа разработана для возрастных категорий 6,5-11 лет, 11-16 лет, 16-18 лет. Направленность дополнительной общеобразовательной программы - техническая.

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 и 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» заключена 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 1-11 классов для трех возрастных категорий по 6 часов (6,5-11 лет, 11-16 лет, 16-18 лет 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 месяц 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 (5-25 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.

Способы определения планируемых результатов - педагогическое наблюдение, тесты, педагогический анализ результатов анкетирования, тестирования, зачётов, взаимозачётов, опросов, выполнения обучающимися диагностических заданий, участия в мероприятиях, защиты проектов, решения задач поискового характера, активности обучающихся на занятиях и т.п. Для отслеживания результативности можно использовать:

-педагогический мониторинг, включающий контрольные задания и тесты, диагностику личностного роста и продвижения, анкетирование, педагогические отзывы, ведение журнала учета или педагогического дневника, ведение оценочной системы;

- мониторинг образовательной деятельности детей, включающий самооценку обучающегося, ведение зачетных книжек, ведение творческого дневника обучающегося, оформление листов индивидуального образовательного маршрута, оформление фотоотчета и т.д.

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.

УЧЕБНО-ТЕМАТИЧЕСКИЙ ПЛАН

(6,5-11 лет)

№ п/п	Тема	Всего часов	Теоретические занятия	Практические занятия
1.	Информация, компьютер и Интернет.	1	1	0
2.	Мир виртуальный и реальный. Интернет зависимость.	1	1	0
3.	Методы безопасной работы в Интернете	1	1	0
4.	Основные правила поведения сетевого взаимодействия	2	1	1
5.	Государственная политика в области защиты информации	1	1	0
	Итого	6	5	1

СОДЕРЖАНИЕ ПРОГРАММЫ

Тема № 1. - 1 ч.

Информация, компьютер и Интернет.

1. Основные вопросы: Компьютер - как он появился, как появился Интернет. Почему компьютер нужно беречь. Где и как искать информацию. Интернет - средство для поиска полезной информации. Как защитить себя от информационной перегрузки. Что такое файл. Как обращаться со своими и чужими файлами, чтобы их не потерять. Какие файлы можно скачивать, а какие нельзя. Полезные и вредные страницы Интернета. Как отличать полезную и правдивую информацию. Ненужные ссылки, ложные ссылки, реклама. Что такое вредоносные сайты. К чему ведет переход по вредоносным ссылкам. Опасная информация в сети. Возьми с собой электронного помощника. Мобильные устройства. Польза и опасности мобильной связи, Общение в Интернете - переписка, форумы, социальные сети. Совместные игры в Интернете. Обмен данными при совместной работе - скайп, IP-телефония, ICQ. Безопасный обмен данными. На каких устройствах можно сохранить информацию и как с ними правильно обращаться (диски, флэш, карты и пр.). Как работать в группе. Как передать товарищам результаты работы и не повредить их компьютерам. Что такое электронная почта.

2. Требования к знаниям и умениям:

Обучающиеся должны знать историю появления компьютера и Интернета. Правила работы с компьютером. Научиться соблюдать правила работы с файлами. Уметь отличать безопасные сайты и ссылки от вредоносных. Знать технические и программные возможности мобильных устройств. Преимущества мобильной связи и их опасность. Понимать пользу и опасности виртуального общения, социальных сетей.

Обучающиеся должны уметь правильно работать с компьютером. Пользоваться браузером для поиска полезной информации. Внимательно прочитывать сообщения о нежелательных страницах, отказываться от их просмотра, выполнять основные действия с файлами. Копировать файлы, проверять файлы на вирусы. Уметь работать с информацией и электронной почтой. Владеть основными приемами поиска информации в сети Интернет.

Тема № 2 . - 1 ч.

Мир виртуальный и реальный. Интернет зависимость.

1. Основные вопросы: Что такое Интернет-сообщество. Как не превратить свою жизнь в виртуальную? Социальные сети. Детские социальные сети. Какую информацию о себе следует выкладывать в сеть? Какая информация принадлежит вам? Не слишком ли много у вас друзей в социальной сети? Что такое интернет-зависимость? Виртуальная личность - что это такое? Сайты знакомств. Незнакомцы в

Интернете. Превращение виртуальных знакомых в реальных. Развлечения в Интернете. Игры полезные и вредные. Признаки игровой зависимости.

2. Требования к знаниям и умениям:

Обучающиеся должны знать виды общения в Интернете. Правила безопасной работы при интернет - общении.

Обучающиеся должны уметь пользоваться основными видами программ для общения в сети. Чего не следует делать при сетевом общении.

Уметь применять программу Skype для общения, создание контактов. Отличать вредные игры от полезных.

Тема № 3 . - 1 ч.

Методы безопасной работы в Интернете.

1. Основные вопросы: Ищите в Интернете только то, что вам требуется. Как защититься от вредного контента. Что такое контент-фильтры, движение в Интернете (серфинг). Знаки Интернета, рассказывающие об опасной информации. Правильно ли работает компьютер? Признаки работы вирусов. Вирусы и антивирусы. Обновление баз. Что такое электронные деньги, как с ними правильно обращаться. Почему родители проверяют, что ты делаешь в Интернете?

2. Требования к знаниям и умениям:

Обучающиеся должны знать основные понятия о компьютерных вирусах и контент-фильтрах.

Обучающиеся должны уметь использовать приемы работы с антивирусными программами, запускать программы-антивируса для сканирования компьютера и внешних носителей информации, устанавливать и сканировать антивирусной программой. Детские контент-фильтры.

Тема № 4 . - 2 ч.

Основные правила поведения сетевого взаимодействия

1. Основные вопросы:

Интернет и экономика - польза и опасность. Кто и как может навредить в Интернете. Электронная торговля - ее опасности. Поиск информации: если у вас требуют личную информацию при скачивании данных. Что такое личная информация. Если вам сообщают о выигрыше в лотерею. Если вам предлагают установить новое приложение. Сколько стоят ошибки в интернете.

2. Требования к знаниям и умениям:

Обучающиеся должны знать принципы работы интернет - магазинов, понятие «электронные деньги». Обучающиеся должны уметь дозировано использовать личную информацию в сети интернет.

Уметь различать (распознавать) мошеннические действия.

3. Тематика практических работ:

Практическая работа №1. Квест «Покупка в интернет-магазине».

Тема №5. -1 ч.

Государственная политика в области защиты информации.

1. Основные вопросы: Как государство защищает киберпространство. Войны нашего времени. Что такое кибервойна. Почему государство защищает информацию. Защита государства и защита киберпространства.

2. Требования к знаниям и умениям:

Обучающиеся должны знать политику государства в области защиты информации.

Обучающиеся должны уметь защищать свои информационные данные от внешнего воздействия (интернет и вирусы, вирусы и злоумышленники).

УЧЕБНО-ТЕМАТИЧЕСКИЙ ПЛАН

(11-16 лет)

№ п/п	Тема	Всего часов	Теоретические занятия	Практические занятия
1.	Общие сведения о безопасности ПК и Интернета	1	1	0
2.	Проблемы Интернет - зависимости	1	1	0
3.	Методы обеспечения безопасности ПК и Интернета. Вирусы и антивирусы.	2	1	1
4.	Мошеннические действия в Интернете. Киберпреступления	1	1	0
5.	Государственная политика в области кибербезопасности. Сетевой этикет.	1	1	0
	Итого	6	5	1

СОДЕРЖАНИЕ ПРОГРАММЫ

Тема № 1. (1 час)

Общие сведения о безопасности ПК и Интернета

1. 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.

2. Требования к знаниям и умениям:

Обучающиеся должны знать как устроен компьютер и интернет, как работают мобильные устройства, какие существуют угрозы для мобильных устройств, что такое защита персональных данных, аспекты кибербезопасности, что такое компьютерная и информационная безопасность, что такое кибертерроризм и кибервойны, основные угрозы безопасности информации.

Обучающиеся должны уметь защищать свои персональные данные, составлять безопасные сети контактов, своевременно обнаружить проблемы сети, восстанавливать параметры систем.

Тема № 2. (1 час)

Проблемы Интернет-зависимости

1. 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).

2. Требования к знаниям и умениям:

Обучающиеся должны знать, что такое ЗОЖ, и как влияет компьютер на здоровье, какое психологическое воздействие оказывает информация на личность человека, критерии зависимости, типы интернет-зависимости, как развивается зависимость.

Обучающиеся должны уметь распознавать и избегать деструктивную информацию в Интернете, уметь вовремя выявить интернет-зависимость и сообщить специалистам.

Тема № 3. (2 часа)

Методы обеспечения безопасности ПК и Интернета. Вирусы и антивирусы.

1. 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.

2. Требования к знаниям и умениям:

Обучающиеся должны знать типы вирусов, что такое антивирусная защита, антивирусные программы, как лечить компьютер, как защитить мобильные устройства, как защитить фото- и видеоматериал от скачиваний.

Обучающиеся должны уметь распознавать вирусы, пользоваться антивирусными защитными программами, соблюдать меры личной безопасности при сетевом общении.

3. Тематика практических работ:

Практическая работа №1. «Установка антивирусной программы»;

Практическая работа №2. Создание презентации на тему: «Разновидности вирусов. Черви, трояны, скрипты», «Шпионские программы». «Шифровальщики». «Троян-вымогатель в социальной сети “ВКонтакте” или наказание для особо любопытных».

Тема № 4. (1 часов)

Мошеннические действия в Интернете. Киберпреступления.

1. 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.

2. 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.

Тема № 5. (1 часов)

Сетевой этикет. Психология и сеть

3. **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)

4. **Требования к знаниям и умениям:**

Обучающиеся должны знать сетевой этикет, этические и правовые нормы информационной деятельности человека, информационный этикет и право, информационную безопасность.

Обучающиеся должны уметь использовать этические и правовые нормы информационной деятельности человека, информационный этикет и право, информационную безопасность

Государственная политика в области кибербезопасности.

1. **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.

2. **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 право, охраны программ для ЭВМ и баз данных(БД), лицензионных программ.

Обучающиеся 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(БД), лицензионных программ.

УЧЕБНО-ТЕМАТИЧЕСКИЙ ПЛАН (16-18 лет)

№ п/п	Тема	Всего часов	Теоретические занятия	Практические занятия
1	Общие сведения о безопасной работе в сети Интернет	1	1	0
2	Проблемы Интернет зависимости	1	1	0
3	Технические аспекты безопасного использования Интернета	1	1	0
4	Мошеннические действия в Интернете.	1	1	0
5	Информационная этика. Информационное право и информационная безопасность в киберпространстве	1	1	0
6	Государственная политика в области кибербезопасности	1	1	0
	Итого	6	6	0

СОДЕРЖАНИЕ ПРОГРАММЫ

Тема № 1 . - 1 ч.
Общие сведения о безопасной работе в сети Интернет

4. Основные вопросы:

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 ресурсам компьютера. Хакерские атаки. Виды хакерских атак. Новые технологии и новые угрозы информационной безопасности (применение робототехники и т.п.). Рост числа угроз для мобильных устройств. Кибершпионаж.

5. 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.

Обучающиеся должны уметь ответственно и безопасно использовать возможности сети интернет для поиска, хранения, использования информации и информационных услуг.

Тема № 2. - 1ч.

Проблемы Интернет - зависимости

3. Основные вопросы:

Классификация интернет - зависимостей и их профилактика.

4. Требования к знаниям и умениям:

Обучающиеся должны знать классификацию интернет - зависимостей и способы профилактики.

Обучающиеся должны уметь классифицировать интернет - зависимости и проводить профилактику.

Тематика практических работ:

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

Тема № 3. - 3 ч.

Технические аспекты безопасного использования Интернета

1. Основные вопросы:

Аппаратная защита ПО и сети (электронные ключи, аппаратные брандмауэры) 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 (Windows, Linux). Онлайн сервисы для безопасности пользователя в интернете (проверка компьютера и файлов на вирусы on-line). Защитное ПО. Антивирусные программы. Межсетевые экраны. Брандмауэры. Как узнать местоположение компьютера по IP-адресу. Способы обеспечения безопасности веб-сайта. Коммерческое и бесплатное антивирусное ПО.

2. Требования к знаниям и умениям:

Обучающиеся должны знать аппаратную защиту ПО и сети, параметры безопасности ПК, защита файловой системы, способы резервного копирования и восстановление данных, признаки заражения компьютерных программ, защитное ПО, антивирусные программы, межсетевые экраны, брандмауэры, способы определения местоположение компьютера по IP-адресу, способы обеспечения безопасности вебсайта.

Обучающиеся 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.

Тема № 4 . - 1 ч.

Мошеннические действия в Интернете.

Основные вопросы:

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

Требования к знаниям и умениям:

Обучающиеся должны знать технику безопасности при регистрации на веб-сайтах, сайтах знакомств, понятия компьютерное пиратство, плагиат, кибернаемники и кибердетективы.

Обучающиеся должны уметь использовать правовые нормы, относящиеся к информации, правонарушениям в информационной сфере, меры их предотвращения, личную информацию, информационную безопасность, информационное право.

Тема № 5 . - 1 ч.

Информационная этика. Информационное право и информационная безопасность вкиберпространстве

Основные вопросы:

Сетевой этикет. Значение сетевого этикета. Ответственность за киберпреступления. Конституционное право на поиск, получение и распространение информации. Федеральный закон от 29.12.2010 N436- ФЗ (ред. от 28.07.2012) "О защите детей от информации, причиняющей вред их здоровью и развитию" (действует с 1 сентября 2012 года). Информационное законодательство РФ. Закон РФ "Об информации, информационных технологиях и о защите информации. "Уголовная ответственность за создание, использование и распространение вредоносных компьютерных программ (ст. 237 УК РФ). Правовая охрана программ для ЭВМ и БД. Коммерческое ПО. Бесплатное ПО (Freeware, Free, FreeGPL, Adware), условно-бесплатное ПО (Trial, Shareware, Demo). Правовые основы для защиты от спама. Правовые основы защиты интеллектуальной собственности. Авторское право. Правовая охрана программ для ЭВМ и баз данных (БД). Лицензионное ПО. Виды лицензий (OEM, FPP, корпоративные лицензии, подписка). ПО с открытым кодом (GNUGPL, FreeBSD).

Требования к знаниям и умениям:

Обучающиеся должны знать сетевой этикет, этические и правовые нормы информационной деятельности человека, информационный этикет и право, информационную безопасность.

Обучающиеся должны уметь использовать этические и правовые нормы информационной деятельности человека, информационный этикет и право, информационную безопасность

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 право, охраны программ для ЭВМ и баз данных (БД), лицензионных программ.

Обучающиеся должны уметь пользоваться правовыми основами защиты от информации, причиняющей вред здоровью и развитию.

Тема №6. - 1ч.

Государственная политика в области кибербезопасности

Основные вопросы:

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.

Обучающиеся должны уметь ориентироваться в Государственной политике в области кибербезопасности.

МЕТОДИЧЕСКОЕ ОБЕСПЕЧЕНИЕ

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 умений и навыков.

При проектировании занятий необходимо придерживаться следующих **принципов** системно-деятельностного подхода:

- принцип активной включенности школьников в освоение предлагаемой информации;
- принцип деятельности;
- принцип доступности;
- принцип системности;
- принцип рефлексивности;
- принцип мотивации;
- принцип открытости содержания образования.

Принцип активной включенности обучающихся в освоение предлагаемой информации предполагает субъектную позицию школьника в образовательном процессе, обращение педагога к личностному опыту учащегося и обогащение его в процессе деятельности на занятии. Важной составляющей в этом случае является создание для школьников условий транслирования информации, полученной в ходе занятий, в принципы собственной жизнедеятельности. Введение деятельностных технологий в обучающий процесс предполагает учет следующих критериев: интерактивность; игровой, театрализованный контекст; совместную деятельность ребенка и взрослого; учет психолого-возрастных особенностей школьников; использование социокультурных технологий.

Принцип доступности предполагает адекватность содержания и подачи предлагаемого материала применительно к возрастным и психологическим особенностям школьников, а также имеющемуся у них социальному опыту.

Принцип системности позволяет целостно представить учащимся как положительные, так и отрицательные стороны использования сети интернет.

Принцип рефлексивности предполагает организацию самостоятельной познавательной деятельности школьников на всех этапах занятий с целью вовлечения их в процесс осмысления полученной информации, соотнесения ее с имеющимся личным социальным опытом и включения приобретенного нового содержания и способов деятельности в собственную практику.

Принцип мотивации. Проектировать занятие таким образом, чтобы мотивировать школьников на самостоятельный поиск новой информации относительно использования инфокоммуникационных технологий в познавательных и развивающих целях, стимулировать их творческие и познавательные мотивационные потребности. Использовать средства побуждающего и формирующего воздействия. Эти средства необходимо применять так, чтобы они способствовали развитию различных компонентов и сторон мотивации в их единстве. Поэтому они должны применяться в комплексе, включающем приемы побуждения: и за счет стимулирующего влияния содержания учебного материала, и за счет побуждающей функции методов обучения, и за счет сочетания различных видов деятельности. Все это в совокупности обеспечит динамику развития положительных потребностно-мотивационных состояний учащихся в соответствии со структурой мотивационной основы деятельности.

Принцип открытости содержания образования предполагает достаточно гибкое использование педагогом предложенной конструкции, не допуская при этом искажения логики, содержательной точности и достоверности информации.

Материально-техническое обеспечение реализации дополнительной общеобразовательной программы «Безопасность в сети Интернет» включает следующий перечень необходимого оборудования:

1. Компьютер;
2. Мультимедийный проектор.
3. Интерактивная доска
4. Доступ к сети Интернет.

ПРИЛОЖЕНИЕ 1

Тест по безопасности в сети Интернет
(6,5-11 лет)

Как могут распространятся компьютерные вирусы?

a. Посредством электронной почты.
b. При просмотре веб-страниц.
c. Через клавиатуру.
d. Их распространяют только преступники.

1. Зачем нужен брандмауэр?

a. Он не дает незнакомцам проникать в компьютер и просматривать файлы.
b. Он защищает компьютер от вирусов.
c. Он обеспечивает защиту секретных документов.
d. Он защищает компьютер от пожара.

2. Всегда ли можно быть уверенным в том, что электронное письмо было получено от указанного отправителя?

a. Да
b. Да, если вы знаете отправителя
c. Нет, поскольку данные отправителя можно легко подделать
d. Может быть.

3. На компьютере отображается непонятное сообщение. Какое действие предпринять?

a. Продолжить, будто ничего не произошло.
b. Нажать кнопку «ОК» или «ДА»
c. Обратится за советом к учителю, родителю или опекуну.
d. Больше никогда не пользоваться Интернетом

4. Что нужно сделать при получении подозрительного сообщения электронной почтой?

a. Удалить его, не открывая.
b. Открыть его и выяснить, содержится ли в нем какая-нибудь важная информация.
c. Открыть вложение, если такое имеется в сообщении.
d. Отправить его родителям

5. В ящик входящей почты пришло «письмо счастья». В письме говорится, чтобы его переслали пяти друзьям. Какое действие предпринять?

a. Переслать его пяти друзьям.
b. Переслать его не пяти друзьям, а десяти друзьям.
c. Не пересылать никакие «письма счастья»

d. Ответить отправителю, что вы больше не хотите получать от него/нее письма.

6. В каких случаях можно, не опасаясь последствий, сообщать в Интернете свой номер телефона или домашний адрес?

a. Во всех случаях.

b. Когда кто-то просит об этом.

c. Когда собеседник в чате просит об этом.

d. Такую информацию следует с осторожностью сообщать людям, которым вы доверяете.

7. Вы случайно прочитали пароль, который ваш друг записал на листочке бумаг. Как вы должны поступить?

a. Запомнить его.

b. Постараться забыть пароль.

c. Сообщить другу, что вы прочитали пароль, и посоветовать сменить пароль и никогда больше не записывать на листе бумаги.

d. Сообщить пароль родителям.

8. Что такое сетевой этикет?

a. Правила поведения за столом.

b. Правила дорожного движения.

c. Правила поведения в Интернете.

d. Закон, касающийся Интернета.

9. Что запрещено в интернете?

a. Запугивание других пользователей.

b. Поиск информации.

c. Игры.

d. Общение с друзьями

ПРИЛОЖЕНИЕ 2.

Тест по безопасности в сети Интернет

(11-16 лет)

«Основы безопасности в Интернете» Осторожно, вирус!

1. Что является основным каналом распространения компьютерных вирусов?
    a. Веб-страницы
    b. Электронная почта
    c. Флеш-накопители (флешки)
2. Для предотвращения заражения компьютера вирусами следует:
    a. Не пользоваться Интернетом
    b. Устанавливать и обновлять антивирусные средства
    c. Не чихать и не кашлять рядом с компьютером
3. Если вирус обнаружен, следует:
    a. Удалить его и предотвратить дальнейшее заражение
    b. Установить какую разновидность имеет вирус
    c. Выяснить как он попал на компьютер
4. Что не дает хакерам проникать в компьютер и просматривать файлы и документы:
    a. Применение брандмауэра
    b. Обновления операционной системы
    c. Антивирусная программа

5. Какое незаконное действие преследуется в России согласно Уголовному Кодексу РФ?
    a. Уничтожение компьютерных вирусов
    b. Создание и распространение компьютерных вирусов и вредоносных программ
    c. Установка программного обеспечения для защиты компьютера

Осторожно, Интернет!

1. Какую информацию нельзя разглашать в Интернете?
    a. Свои увлечения
    b. Свой псевдоним
    c. Домашний адрес
2. Чем опасны социальные сети?
    a. Личная информация может быть использована кем угодно в разных целях
    b. При просмотре неопознанных ссылок компьютер может быть взломан
    c. Все вышеперечисленное верно
3. Виртуальный собеседник предлагает встретиться, как следует поступить?

a. Посоветоваться с родителями и ничего не предпринимать без их согласия

b. Пойти на встречу одному

c. Пригласить с собой друга

4. Что в Интернете запрещено законом?

a. Размещать информацию о себе

d. Размещать информацию других без их согласия

c. Копировать файлы для личного использования

5. Действуют ли правила этикета в Интернете?

a. Интернет - пространство свободное от правил

b. В особых случаях

c. Да, как и в реальной жизни

ПРИЛОЖЕНИЕ 3.

Тест по безопасности в сети Интернет
(16-18 лет)

1. Когда можно полностью доверять новым онлайн-друзьям?
   a) Ничто не может дать 100%-ную гарантию того, что онлайн-другу можно доверять
   b) Поговорив по телефону
   c) После обмена фотографиями
   d) Когда есть общие друзья
   e) После длительного онлайн-знакомства (переписки)

2. Что делать, если ты столкнулся с троллем в Сети?
   a) Сообщить модераторам сайта
   b) Рассказать взрослым
   c) Игнорировать выпады тролля
   d) Заблокировать тролля
   e) Проучить или доказать свою правоту

3. Как пожаловаться на неприемлемый контент на YouTube?
   a) Выразить свое недовольство в комментариях к видео
   b) Отметить видео “флажком”, который находится под ним
   c) Такого функционала нет
   d) Найти электронный адрес автора видео и написать ему сообщение

4. Что является признаком фишинг-сообщения?
   a) В сообщении много ошибок, неточностей и противоречий
   b) Сообщение содержит обещание большой выгоды с минимальными усилиями
   c) В сообщении требуется срочно сменить пароль от электронной почты по причине вероятной попытки взлома электронного ящика, при этом сообщение не отправлено с официального адреса почтовой службы
   d) В сообщении запрашиваются твои личные данные, финансовая информация, пароли
   e) Сообщение содержит угрозу для жизни и здоровья близких людей

5. Как обезопасить себя при первой встрече с онлайн-другом?
   a) Заранее пообщаться с “незнакомцем” по телефону, попросить прислать фотографии, таким образом убедиться, что он тот, за кого себя выдает.
   b) Убедиться, что у вас есть общие увлечения и темы для разговора в реальной жизни.
   c) Встречаться с интернет-незнакомцами очень опасно, лучше не назначать

встречу, если не знакомы с человеком лично.

d) Попросить присутствовать взрослых.
e) Сообщить о встрече родителям/взрослым, спросить их совета.
f) Взять на встречу друзей и выбрать людное место в светлое время суток.

6. Где можно найти информацию для реферата в Интернете?
   a) На сайтах средств массовой информации
   b) В электронной библиотеке
   c) В поисковой системе
   d) В Википедии

7. Какую информацию о себе опасно выкладывать в Интернете в открытом доступе?
   a) Дату рождения
   b) О своих интересах
   c) Информацию о доходах родителей
   d) Домашний адрес и телефон
   e) Место работы родителей

8. Как пожаловаться на неприемлемый контент на YouTube?
   a) Отметить видео “флажком”, который находится под ним
   b) Такого функционала нет
   c) Выразить свое недовольство в комментариях к видео
   d) Найти электронный адрес автора видео и написать ему сообщение

9. Что делать, если вы стали жертвой интернет-мошенничества?
   a) Сообщить взрослым
   b) Сменить все пароли
   c) Попробовать решить проблему самостоятельно
   d) Позвонить на Линию помощи «Дети онлайн»

10. Как нужно себя вести, если вы стали жертвой кибербуллинга?
    a) Обратиться за поддержкой к модераторам сайта
    b) Пытаться бороться с обидчиками в одиночку
    c) Заблокировать обидчиков
    d) Сообщить родителям/взрослым
    e) Ничего не делать
    f) Обратиться на Линию помощи «Дети онлайн»

11. Как защититься от негативного контента?
    a) Установить программы родительского контроля
    b) Сообщить модераторам сайта, пожаловаться на неприемлемый контент с помощью специальных инструментов, доступных на сайте

c) Обратиться к автору негативного контента
d) Не обращать на него внимания
e) Использовать безопасный поиск Googleи безопасный режим на YouTube
f) рос:

12. Что следует делать, если на сайте вас просят отправить бесплатное сообщение на короткий номер?
a) Как можно быстрее отправить СМС
b) Постараться найти стоимость СМС на сайте, после этого поискать в интернете, какова стоимость отправки СМС на этот номер, и перепроверить эту информацию. До перепроверки информации не отправлять СМС
c) Использовать телефон друга или знакомого чтобы, отправить СМС

13. Что делать, если ты столкнулся с троллем в Сети?
a) Игнорировать выпады тролля
b) Проучить или доказать свою правоту
c) Заблокировать тролля
d) Рассказать взрослым
e) Сообщить модераторам сайта

14. Как защитить свою электронную почту от взлома и махинаций?
a) Регулярно менять пароли
b) Активировать систему двухэтапной верификации на сервисах, которые позволяют это сделать
c) Никому не сообщать свой пароль
d) Периодически менять адрес электронной почты, менять провайдеров
e) Не открывать сообщения с незнакомых и подозрительных адресов
f) Создавать разные пароли от разных аккаунтов, включая электронную почту, систему электронного банкинга и пр.

15. При каких условиях можно доверять письму от неизвестного отправителя?
a) Никогда нельзя доверять письму от неизвестного отправителя
b) К вам обращаются по имени
c) Отправитель использует логотип авторитетной компании
d) Письмо содержит важную информацию о ваших близких
e) Отправитель ссылается на ваших друзей

16. Что делать, если вам пришло письмо о том, что вы выиграли в лотерее?
a) Отметить сообщение как спам
b) Перейти по ссылке в письме, ведь в редких случаях информация может оказаться правдой
c) Удалить его

d) Заблокировать отправителя
e) Написать в ответ разоблачающее письмо мошенникам

17. Что делать, если вам приходит сообщение по электронной почте или во всплывающих окнах о том, что ваш компьютер заражён?
a) Пройти по предлагаемым ссылкам и скачать антивирусную систему
b) Закрыть всплывающее окно и не нажимать на ссылки в нём
c) Просканировать компьютер на возможные вирусы, при этом не переходить по незнакомым ссылкам

18. Как защитить компьютер от атак вредоносных программ?
a) Никогда не переходить по ссылкам из всплывающих окон
b) Перед запуском проверять все файлы, скачанные из Интернета, с помощью антивируса
c) Регулярно обновлять браузер, операционную систему, антивирусную программу и прикладное программное обеспечение
d) Установить на компьютер сразу несколько антивирусных программ
e) Установить антивирусную программу с официального сайта
f) Не открывать вложения в письмах, присланных с неизвестных электронных адресов, а также с осторожностью относиться к письмам, которые пришли с известного вам адреса, но чье содержание кажется подозрительным: аккаунт ваших знакомых может быть взломан и содержать вирусы

19. Какие функции браузера не следует использовать на общественном компьютере?
a) Безопасный поиск
b) Автозаполнение форм
c) Автосохранение паролей
d) Режим инкогнито

20. В каком случае нарушается авторское право?
a) При размещении на YouTubeсобственного видеоролика с концерта любимой группы
b) При использовании материалов Википедии для подготовки реферата со ссылкой на источник
c) При размещении не лицензионного контента в социальных сетях
d) При просмотре не лицензионного контента в социальных сетях
e) При чтении романа Л.Н. Толстого «Война и мир» в Интернете

21. Что в Интернете запрещено законом?
a) Размещать информацию о себе
b) Размещать информацию других без их согласия
c) Копировать файлы для личного использования

22. Действуют ли правила этикета в Интернете?
    a) Интернет - пространство свободное от правил
    b) В особых случаях
    c) Да, как и в реальной жизни
23. Чем опасны социальные сети?
    a) Личная информация может быть использована кем угодно в разных целях
    b) При просмотре неопознанных ссылок компьютер может быть взломан
    c) Все вышеперечисленное верно
24. Что не дает хакерам проникать в компьютер и просматривать файлы и документы:
    a) Применение брандмауэра
    b) Обновления операционной системы
    c) Антивирусная программа
25. Какое незаконное действие преследуется в России согласно Уголовному Кодексу РФ?
    a) Уничтожение компьютерных вирусов
    b) Создание и распространение компьютерных вирусов и вредоносных программ
    c) Установка программного обеспечения для защиты компьютера

СПИСОК ЛИТЕРАТУРЫ

Нормативно правовые документы:

1. Федеральный закон «О защите детей от информации, причиняющей вред их здоровью и развитию» от 29 декабря 2010 г. № 436-ФЗ - https://rg.ru/2010/12/31/deti-inform-dok.html;
2. Федеральный закон Российской Федерации от 21 июля 2011 г. № 252-ФЗ «О внесении изменений в отдельные законодательные акты Российской Федерации в связи с принятием Федерального закона «О защите детей от информации, причиняющей вред их здоровью и развитию» - http://base. garant.ru/12188176/;
3. Федеральный закон от 29.12.2012 г. № 273-ФЗ «Об образовании в Российской Федерации» (с изм., внесенными Федеральными законами от 04.06.2014 г. № 145-ФЗ, от 06.04.2015 г. № 68-ФЗ) // http: //www. consultant. ru/;http: //www. garant. ru/
4. Федеральный государственный образовательный стандарт начального общего образования (1-4 классы) (Приказ Министерства образования и науки РФ от 6 октября 2009 г. N373 "Об утверждении и введении в действие федерального государственного образовательного стандарта начального общего образования" С изменениями и дополнениями от: 26 ноября 2010 г., 22 сентября 2011 г., 18 декабря 2012 г., 29 декабря 2014 г., 18 мая, 31 декабря 2015 г.http://base, garant.ш/197127/#ixzz4tOU3n8rF);
5. Федеральный государственный образовательный стандарт начального общего образования обучающихся с ограниченными возможностями здоровья (Приказ Министерства образования и науки РФ от 19 декабря 2014 г. N1598 "Об утверждении федерального государственного образовательного стандарта начального общего образования обучающихся с ограниченными возможностями здоровья"http://base.garant.ni/70862366/#ixzz4tOz0KaU21;
6. Федеральный компонент государственных образовательных стандартов начального общего, основного общего и среднего (полного) общего образования (1-4 классы) (с изменениями на 7 июня 2017 года).
7. Приказ Министерства образования и науки Российской Федерации от 30.08.2013 г. № 1015 (в ред. Приказов Минобрнауки России от 13.12.2013 г. №1342, от 28.05.2014 г. № 598, от 17.07.2015 г. № 734) «Об утверждении Порядка организации и осуществления образовательной деятельности по основным общеобразовательным программам - образовательным программам начального общего, основного общего и среднего общего образования» (Зарегистрировано в Минюсте России 01.10.2013 г. № 30067) // http://www.consultant.nl/; http://www.garant.ru/
8. Приказ Министерства образования и науки Российской Федерации № 336 от 30.03.2016 «Об утверждении средств обучения и воспитания, необходимых для реализации образовательных программ начального общего, основного общего и среднего общего образования, соответствующих современным условиям обучения, необходимого для оснащения образовательных организаций, в целях реализации мероприятий

по содействию созданию в
субъектах Российской Федерации (исходя из прогнозируемой потребности) новых мест в общеобразовательных организациях, критериев его формирования и требований к функциональному оснащению, а так же норматива стоимости оснащения одного места http: //минобрнауки. рф/документы/8163

9. Приказ Минобрнауки России от 15 июня 2016 г. № 715 «Об утверждении Концепции развития школьных информационно-библиотечных центров» // http: //www. consultant. ru/;http: //www. garant. ru/
10. Постановление Главного государственного санитарного врача Российской Федерации от 29.12.2010 № 189 (ред. от 25.12.2013 г.) «Об утверждении СанПиН 2.4.2.2821-10 «Санитарно-эпидемиологические требования к условиям и организации обучения в общеобразовательных учреждениях» (Зарегистрировано в Минюсте России 03.03.2011 г. № 19993), (в ред. Изменений № 1, утв. Постановлением Главного государственного санитарного врача Российской Федерации от 29.06.2011 № 85, Изменений № 2, утв. Постановлением Главного государственного санитарного врача Российской Федерации от 25.12.2013 г. № 72, Изменений № 3, утв. Постановлением Главного государственного санитарного врача РФ от 24.11.2015 г. №81) // http://www.consultant.ru/; http://www.garant.nl/
11. Постановление Главного государственного санитарного врача Российской Федерации от 10.07.2015 г.№ 26 «Об утверждении СанПиН 2.4.2.3286-15«Санитарно- эпидемиологические требования к условиям и организации обучения и воспитания в организациях, осуществляющих образовательную деятельность по адаптированным основным общеобразовательным програм мам для обучающихся с ограниченными возможностями здоровья» (Зарегистрировано в Минюсте России 14.08.2015 г. № 38528) // http://www.consultant.ru/; http://www.garant.ru/

***Основная литература*:**

1. Бирюков А. А. Информационная безопасность защита и нападение 2е издание: Издательство: ДМК-Пресс., 2017, 434 с.
2. Бирюков А.А. Информационная безопасность защита и нападение.: Издательство: ДМК-Пресс., 2012, 474 с.
3. Колесниченко Денис. Анонимность и безопасность в интернете. От чайника к пользователю. Самоучитель Издательство: БХВ-Петербург, 2012, 240с.
4. Мазаник Сергей. Безопасность компьютера. Защита от сбоев, вирусов и неисправностей: издательство: ЭКСМО, 2014, 256 с.
5. Мэйволд Э. Безопасность сетей (2-е изд.) Книги» Сетевые Технологии. Название: Безопасностьсетей: Издательство: М.: НОУ "Интуит", 2016,571 с.
6. Платонов В.В. Программноаппаратные средства защитыинформации: учебник для студ. Учрежд.высш. проф. образования / В. В.Платонов. — М.: Издательский центр «Академия», 2013,336 с.
7. Проскурин В.Г Защита в операционных системах: Издательство: Горячая

линия-Телеком, 2014, 192 с.

8. Савченко Е. Кто, как и зачем следит за вами через интернет: Москва - Третий Рим, 2012, 100 с.
9. Яковлев В.А. Шпионские и антишпионские штучки: Техническая литература Издательство: Наука и Техника, 2015, 320 с.

Дополнительная:

1. "Березовый лес" или "лес березовый" /П. Лауфер//Юный эрудит. - 2014. - № 3. - С. 24-26
2. Доценко С.М., Шпак В.Ф. Комплексная информационная безопасностьобъекта. От теории к практике, Издательство: ООО «Издательство Полигон», 2000, 215 с.
3. Клепа и железный друг//Клепа. - 2014. -№ 8. - С. 1-33.Электронная версия журнала:http://klepa.ru.
4. Методическое пособие для работников системы общего образования Солдатова Г., Зотова Е., Лебешева М., Шляпников В. «Интернет: возможности, компетенции, безопасность», 2015 - 156с.
5. Сорокина Е.В., Третьяк Т.М. Здоровье и безопасность детей в мире компьютерных технологий и Интернет. [Текст] Учебно-методический комплект. - М.: СОЛОНПРЕСС, 2010. - 176 с.: ил
6. Ццрлов В.Л. Основы информационной безопасности автоматизированных систем. Краткий курс. - Феникс, 2008.

Интернет ресурсы

Полезные ссылки для учителя:

1) http://www.kasperskv.ru- антивирус «Лаборатория Касперского»;
2) http://www.onlandia.org.ua/rus/- безопасная web-зона;
3) http://www.intemeshka.net- международный онлайн-конкурс по безопасному использованию Интернета;
4) Рыжков В.И. Методика преподавания информатики// http://nto.immpu.sgu.rU/sites/default/files/3/ 12697.pdf:
5) http: //www. saferintemet.m- портал Российского Оргкомитета по безопасному использованию Интернета;
6) http://content-filtering.ru- Интернет СМИ «Ваш личный Интернет»;
7) http://www.rgdb.ru- Российская государственная детская библиотека
8) http://www. saferintemet.ш/- Безопасный Интернет. Портал Российского Оргкомитета по проведению Г ода Безопасного Интернета. Мероприятия, Интернет и законодательство, проблемы и решения, международные ресурсы;
9) http://www. safemnet.ru/- Центр Безопасного Интернета в России. Сайт посвящен проблеме безопасной, корректной и комфортной работы в Интернете. Интернет-угрозы и эффективное противодействием им в отношении пользователей;
10) http://www.fid.su/- Фонд развития Интернет. Информация о проектах, конкурсах, конференциях и др. по компьютерной безопасности и безопасности

Интернета;

11) http: //www. micro soft. com/Rus/athome/securitv/kids/etusivu. html - Безопасность в Интернете. "Основы безопасности детей и молодежи в 30 Интернете" — интерактивный курс по Интернет-безопасности, предлагаемый российским офисом Microsoftв рамках глобальных инициатив Microsoft"Безопасность детей в Интернете" и "Партнерство в образовании". В разделе для учащихся (7-16 лет) предлагается изучить проблемы информационной безопасности посредством рассказов в картинках. В разделе для родителей и учителей содержится обновленная информация о том, как сделать Интернет для детей более безопасным, а также изложены проблемы компьютерной безопасности;

12) http://www.ifap.ru

Полезные ссылки для обучающихся:

1) http://www. Symantec, com/ru/m/norton/clubsymantec/librarv/article. isp?aid=csteachkids - ClubSymanteceдиный источник сведений о безопасности в Интернете. Статья для родителей «Расскажите детям о безопасности в Интернете». Информация о средствах родительского контроля;

2) http://www.nachalka.com/bezopasnost- Nachalka.comпредназначен для учителей, родителей, детей, имеющих отношение к начальной школе. Статья «Безопасность детей в Интернете». Советы учителям и родителям;

3) http://www.obzh.info/novosti/novoe/bezopasnost-detei-v-intemete.html- Личная безопасность. Основы безопасности жизни. Рекомендации взрослым: как сделать посещение Интернета для детей полностью безопасным;

4) http://www.ifap.ru/1 ibrarv/book099.pdf- «Безопасность детей в Интернете», компания Microsoft. Информация для родителей: памятки, советы, рекомендации;

5) http: //www. intemeshka. net/children/index, phtml- «Интернешка» - детский онлайн-конкурс по безопасному использованию сети Интернет. Советы детям, педагогам и родителям, «полезные ссылки». Регистрация и участие в конкурсе по безопасному использованию сети Интернет;

6) http://www.oszone.net/6213/ - OS.zone.net- Компьютерный информационный портал. Статья для родителей «Обеспечение безопасности детей при работе в Интернет». Рекомендации по программе «Родительский контроль»;

7) http: //www. rgdb. ш/innocuous-intemet - Российская государственная детская библиотека. Ресурс для детей и родителей. Правила безопасного Интернета. Обзор программных продуктов для безопасного Интернета. Как защититься от Интернет-угроз. Ссылки на электронные ресурсы, информирующие об опасностях и защите в Сети;

8) https://www.google.nl/safetvcenter/families/start/basics/- Центр

безопасности. Краткие рекомендации помогут обеспечить безопасность членов семьи в Интернете, даже если вечно не хватает времени;

9) https://ege.vandex.ш/securitv/- Тесты по безопасности;

10) http://www. slideshare.net/shperk/ss-47136465- Безопасность в Интернете. Анатолий Шперх;

11) http: //shperk. ru/v-seti/prokrustovo-lozhe. html- Прокрустово ложе для информационной картины. Как мы читаем тексты в интернете;

12) http://shperk.ru/sovetv/avtoritet.html- Как отличить фейк от настоящего материала? Дело о летающем дьяке Крякутном;

13) http://habrahabr.ru/company/mailru/blog/252091/- Советы по безопасности.

http://www.ifap.ru

Полезные ссылки для взрослой аудитории. Социальные ролики

1. Вы знаете, что делают ваши дети в Интернете?

http: //www. youtube. сот/watch? v=d2 OwtGPEdh4&feature=related

2. Защищайте детей в Интернете

http: //www. youtube. com/watch?v=bdnXmT pZX04&feature=related

3. Линия помощи "Дети онлайн

"http: //www. youtube. com/watch?v=q ivz 1 wJoxk4

4. А что Ваш ребенок видит в Сети?

http: //www. youtube. сот/watch? v=duiiF q oGI 1 U&feature=related

5. Воздействие на детей

http://www. youtube .com/watch? v=8nc ISb9C8g&feature=related