Муниципальное автономное общеобразовательное учреждение
«Лицей № 46» городского округа город Уфа Республики Башкортостан

Рассмотрено	Согласовано	Утверждаю
Руководитель МО(кафедры)	Заместитель директора по УВР	Директор МАОУ «Лицей № 46 »
_____	_____	_____ /Ерёмина Г.А. /
Протокол № 1 от		Приказ № 330 от
«31» авг. 20 г.	«30» 08 2018г.	«30» 08 2018г.

РАБОЧАЯ ПРОГРАММА ПО КУРСУ

«БЕЗОПАСНОСТЬ В СЕТИ ИНТЕРНЕТ»

Класс 5а

на 2018-2019 учебный год

Разработала:
учитель высшей категории
Ишанова Ирина Романовна

Уфа, 2018 г.

ПОЯСНИТЕЛЬНАЯ ЗАПИСКА

Рабочая программа для 5-го класса по «Безопасность в сети Интернет» составлена на основе дополнительной общеобразовательной программы «Безопасность в сети Интернет» ГАУ ДПО Институт Развития Образования Республики Башкортостан (для обучающихся 2-11 классов с учетом уровней образования, срок реализации 1 год). Дополнительная 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".

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.

Рабочая программа курса рассчитана на 35 часов в год, поскольку на изучение курса в основной школе отводится 1 час в неделю

Используемый УМК:

1. Дополнительная общеобразовательная программа «Безопасность в сети Интернет» ГАУ ДПО ИРО РБ.

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.

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.

УЧЕБНО-ТЕМАТИЧЕСКИЙ ПЛАН

(основное общее образование)

№ п/п	Тема	Всего часов	Теоретические занятия	Практические занятия
1.	Общие сведения о безопасности ПК и Интернета	5	4	1
2.	Техника безопасности и экология	5	4	1
3.	Проблемы Интернет - зависимости	5	4	1
4.	Методы обеспечения безопасности ПК и Интернета. Вирусы и антивирусы.	6	4	2
5.	Мошеннические действия в Интернете. Киберпреступления	5	4	1
6.	Сетевой этикет. Психология и сеть	5	4	1
7.	Государственная политика в области кибербезопасности	5	4	1
	Итого:	**36**	**28**	**8**

СОДЕРЖАНИЕ ПРОГРАММЫ
(основное общее образование)
Тема № 1. (5 часов)
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.
3. Тематика практических работ:
1. Практическая работа. Составить информационный буклет «Моя безопасная сеть» или сделать групповую газету «Безопасность в Интернет».
Тема № 2. (5 часов)
Техника безопасности и экология
1. 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
2. Требования к знаниям и умениям:
Обучающиеся должны знать правила поведения в компьютерном классе, как применяются компьютер и мобильные устройства в чрезвычайных ситуациях, какое влияние оказывает компьютер на зрение, какое воздействие оказывают радиоволны на здоровье человека и окружающую среду. Обучающиеся должны уметь соблюдать требования ТБ при работе с компьютером, соблюдать гигиенические требования, проводить комплекс упражнений при работе за компьютером.

3. Тематика практических работ:
Практическая работа. Создание буклета «Техника безопасности при работе с компьютером».

Тема № 3. (5 часов)

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.

3. Тематика практических работ:
Практическая работа. «Создание мультимедийной презентации «ПК и ЗОЖ. Организация рабочего места».

Тема № 4. (6 часов)

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 видеоматериалов 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 № 5. (5 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.

3. Тематика практических работ:

Практическая работа. Доклад на тему: «Правила поведения в сети с мошенниками и злоумышленниками», или «Как не стать жертвой сетевых шуток и розыгрышей».

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)

5. 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

6. Тематика практических работ:

Практическая работа. «Выпуск видеоролика на тему «Как не испортить себе настроение при общении в Сети и не опуститься до уровня «веб-агрессора».

Тема №7. (5 часов)

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.

1. Тематика практических работ:

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

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

КАЛЕНДАРНО-ТЕМАТИЧЕСКОЕ ПЛАНИРОВАНИЕ

№ урока	Раздел, тема урока	Дата проведения	
		план	факт
			5а

Общие сведения о безопасности ПК и Интернета (5 ч)			
1	Техника безопасности и организация рабочего места. Как устроен компьютер и Интернет.	2 нед. сент	
2	Защита персональных данных, почему она нужна.	3 нед. сент	
3	Защита киберпространства.	4 нед. сент	
4	Основные угрозы безопасности информации.	5 нед. сент	
5	Практическая работа №1. Сделать газету «Безопасность в Интернет»	1 нед. окт.	
Техника безопасности и экология (5ч)			
6	Компьютер и мобильные устройства в чрезвычайных ситуациях.	2 нед. окт.	
7	Воздействие радиоволн на здоровье и окружающую среду.	3 нед. окт.	
8	Техника безопасности при работе с компьютером.	4 нед. окт.	
9	Компьютерная техника и экология.	2 нед. нояб.	
10	Практическая работа №2. Создание буклета «Техника безопасности при работе с компьютером»	3 нед. нояб.	
Проблемы Интернет – зависимости (5ч)			
11	Деструктивная информация в Интернете- как ее избежать.	4 нед. нояб.	
12	Психологическое воздействие информации на человека.	5 нед. нояб.	
13	Управление личностью через сеть.	2 нед. дек.	
14	Интернет и компьютерная зависимость.	3 нед. дек.	
15	Практическая работа №3. Создание презентации «ПК и ЗОЖ. Организация рабочего места»	4 нед. дек.	
Методы обеспечения безопасности ПК и Интернета. Вирусы и антивирусы (6 ч).			
16	Компьютерные вирусы.	5 нед. дек.	
17	Инструктаж по технике безопасности на рабочем месте.	3 нед. янв.	
18	Организационные, юридические меры защиты.	4 нед. янв.	
19	Меры защиты ПК, аккаунтов, мобильных устройств.	5 нед. янв.	
20	Практическая работа №4. «Установка антивирусной программы»	2 нед. фев.	
21	Практическая работа №5. Создание презентации на тему «Вирус»	3 нед. фев.	

Мошеннические действия в Интернете. Киберпреступления. (5 ч).			
22	Виды интернет- мошенничества.	4 нед. фев.	
23	Мошенничество при распространении «бесплатного» ПО.	5 нед. фев.	
24	Опасности мобильной связи.	2 нед. мар.	
25	Технология манипулирования в интернете.	3 нед. мар.	
26	Практическая работа №6. Доклад «Правила поведения в сети с мошенниками и злоумышленниками».	4 нед. мар.	
Сетевой этикет. Психология и сеть (5ч)			
27	Что такое этикет. Этика и безопасность	1 нед. апр.	
28	Безопасная работа в сети.	2 нед. апр.	
29	Психологическая обстановка в Интернете.	3 нед. апр.	
30	Психологическая обстановка в Интернете.	4 нед. апр.	
31	Практическая работа №7. Видеоролик на тему «Как не испортить себе настроение в Сети и не опуститься до уровня «веб- агрессора»	1 нед. май	
Государственная политика в области кибербезопасности (4ч)			
32	Собственность в Интернете.	2 нед. май	
33	Защита прав потребителей при использовании услуг Интернета.	3 нед. май	
34	Доктрина информационной безопасности.	4 нед. май	
35	Практическая работа №8. «Буклет Правовые основы для защиты от спама»	5 нед. май	

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. №2 252-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. N 373 "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.ru/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. N 1598 "Об утверждении федерального государственного образовательного стандарта начального общего образования обучающихся с ограниченными возможностями
здоровья" http: //base .garant.ru/70862366/#ixzz4tOz0KaU2);
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.ru/; 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.ru/
11. Постановление Г лавного 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/
12. Закон «Об образовании в Республике Башкортостан» от 1 июля 2013 года № 696-з принятый Государственным собранием-Курултаем Республики Башкортостан 27 июня 2013 года. (с изменениями и дополнениями от 26.12.2014 г., от 27.02.2015 г., 01.07.15 г., 18.09.15 г.)
13. Государственная программа "Развитие образования в Республике Башкортостан"», утверждённая постановлением Правительства Республики Башкортостан от 21 февраля 2013 года № 54.
14. Концепция развития электронного образования в Республике Башкортостан на период 2015-2020 годов.

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 безопасность объекта. 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. Цирлов В.Л. Основы информационной безопасности автоматизированных систем. Краткий курс. - Феникс, 2008.

Интернет ресурсы

Полезные ссылки для учителя:

1) http: //www.kaspersky .ru - антивирус «Лаборатория Касперского»;
2) http://www.onlandia.org.ua/rus/ - безопасная web-зона;
3) http: // www.interneshka.net - международный онлайн-конкурс по безопасному использованию Интернета;
4) Рыжков В.Н. Методика преподавания информатики// http://nto.immpu.sgu.ru/sites/default/files/3/ 12697.pdf;
5) http://www.saferinternet.ru - 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.saferinternet.ru/ - Безопасный Интернет. Портал Российского Оргкомитета по проведению Года Безопасного Интернета. Мероприятия, Интернет и законодательство, проблемы и решения, международные ресурсы;
9) http://www.saferunet.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.microsoft.com/Rus/athome/security/kids/etusivu. html - Безопасность в Интернете. "Основы безопасности детей и молодежи в 30 Интернете"
— интерактивный курс по Интерент-безопасности, предлагаемый российским офисом

Microsoft в 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/ru/norton/clubsymantec/library/article.j sp?aid=c
s_teach_kids - ClubSymantec единый 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.com предназначен 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-internete.html - Личная безопасность. Основы безопасности жизни. Рекомендации взрослым: как сделать посещение Интернета для детей полностью безопасным;
4) http://www.ifap.ru/library/book099.pdf - «Безопасность детей в Интернете», компания Microsoft. Информация для родителей: памятки, советы, рекомендации;
5) http: //www.interneshka.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 .ru/innocuous-internet - 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.ru/safetycenter/families/start/basics/ - Центр

безопасности. Краткие рекомендации помогут обеспечить безопасность членов семьи
в Интернете, даже если вечно не хватает времени;
9) https://ege.yandex.ru/security/ - 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/sovety/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.com/watch?v=d2OwtGPEdh4&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=qivz 1 wJoxk4
4. А что Ваш ребенок видит в Сети?
http: //www.youtube.com/watch?v=duiiFqoGI1U&feature=related
5. Воздействие на детей
http://www.youtube.com/watch?v=8nc ISb9C8g&feature=related

Лист корректировки рабочей программы

Предмет «Безопасность в сети Интернет»

Класс 5а

Учитель Ишанова Ирина Романовна

2018 – 2019 учебный год

№ урока	Тема	Количество часов		Причина корректировки	Способ корректировки
		по плану	дано		