

**МУНИЦИПАЛЬНОЕ БЮДЖЕТНОЕ ОБЩЕОБРАЗОВАТЕЛЬНОЕ УЧРЕЖДЕНИЕ
«СИБИРСКАЯ СРЕДНЯЯ ОБЩЕОБРАЗОВАТЕЛЬНАЯ ШКОЛА №1»
ОМСКОГО МУНИЦИПАЛЬНОГО РАЙОНА ОМСКОЙ ОБЛАСТИ**

**ЦЕНТР ОБРАЗОВАНИЯ ЦИФРОВОГО И ГУМАНИТАРНОГО ПРОФИЛЕЙ
«ТОЧКА РОСТА»**

РАССМОТРЕНО

на педагогическом совете

МБОУ «Сибирская СОШ №1»

Протокол №8 от 30.08.2024 г.

УТВЕРЖДАЮ

Директор МБОУ «Сибирская СОШ №1»

_____ Е.А.Стоянова

Приказ № 70 от 30.08.2024 г.

**Дополнительная общеобразовательная
общеразвивающая программа
«Информационная безопасность»**

Направленность: техническая

Целевая группа: 10 - 16 лет

Сроки реализации: 72 часа (1 год)

Форма реализации: очная

Уровень сложности содержания: стартовый

Автор-составитель:

Екимова Алёна Васильевна

ПОЯСНИТЕЛЬНАЯ ЗАПИСКА

Исследование проблемы безопасности детей 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).

Рабочая программа внеурочной деятельности «Безопасность в сети Интернет» разработана в связи с возросшей потребностью обеспечения информационной безопасности детей при организации урочной и внеурочной деятельности.

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 рабочей программы «Информационная безопасность» заключена в достижении метапредметных результатов и предметных умений дисциплины «Информатика и ОБЖ» 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.

Данная рабочая программа рассчитана для обучающихся 5-10 классов. Объем 72 часа в год.

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.

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.

Формы проведения занятий:

Формы организации деятельности: групповая, индивидуальная, индивидуально

- групповая (3-5 человек). Занятия проводятся в комбинированной, теоретической и практической форме:

- теоретические занятия: основы безопасного поведения при работе с компьютерными программами, информацией в сети интернет, изучение терминов, беседы, лекции;

- практические занятия: работа с мобильными устройствами; 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 программы по внеурочной деятельности «Информационная безопасность» 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

№	Тема	Всего часов	Теоретические занятия	Практические занятия
1	Интернет. Введение в информационную безопасность	15	13	2
2	Угрозы и риски в сети Интернет	10	7	3
3	Безопасное поведение в Интернете	10	8	2
4	Социальные сети и общение в сети	10	7	3
5	Киберзависимость и ее виды	10	9	1
6	Интернет-продажи и Маркетплейсы	10	8	2
7	Как уберечь себя и близких от мошенников	5	3	2
8	Подведение итогов	2	1	1
Итого		72	56	16

СОДЕРЖАНИЕ ПРОГРАММЫ

Тема № 1. - 15ч

Интернет. Введение в информационную безопасность

Основные вопросы: Компьютер – как он появился, как появился Интернет. Интернет. Правила работы с ПК, электронными и мобильными устройствами. Сколько времени можно проводить за компьютером. Что такое информационная безопасность? Определение и важность информационной безопасности. Зачем нужна информационная безопасность? Последствия нарушений информационной безопасности. Роль информационной безопасности в повседневной жизни. Кто отвечает за информационную безопасность? Обязанности пользователей. Технологии и инструменты защиты информации: Антивирусные программы, брандмауэры

и другие средства. Обзор актуальных технологий для защиты личных данных.

Требования к знаниям и умениям:

Обучающиеся должны знать об истории 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 за 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.

Тематика практических работ:

Практическая работа №. 1. Провести SWOT-анализ сети интернет

Практическая работа №. 2. Разработайте рекомендации по созданию надёжных паролей.

Тема № 2. - 10ч

Угрозы и риски в сети Интернет

Основные вопросы: Что такое угрозы в сети Интернет? Определение и классификация угроз (вредоносное ПО, фишинг, социальная инженерия). Основные виды угроз в цифровом пространстве. Взаимосвязь между угрозами и рисками. Каковы наиболее распространенные угрозы? Обзор основных типов угроз: вирусы, трояны, шпионские программы. Определение термина «риск» в контексте информационной безопасности. Как минимизировать угрозы и риски? Основные меры предосторожности (пароли, обновления ПО, использование VPN). Роль пользовательского поведения в снижении рисков. Законодательство и защита пользователей: Как законодательство защищает пользователей от киберугроз? Обзор основных законов и норм в сфере кибербезопасности.

Требования к знаниям и умениям: Обучающиеся должны знать основные правила работы с ПК, электронными книгами и мобильными устройствами в условиях окружающей среды, основные навыки ухода за ПК, опасности при работе с электрическими приборами. Обучающиеся должны уметь соблюдать технику безопасности и гигиену при работе за ПК. Владеть основными приемами навигации в файловой системе.

Тематика практических работ: 3

Практическая работа №. 1. Изучение маркеров фишингового письма и поиск различий между настоящим письмом и фальшивым.

Практическая работа №. 2. Создать короткий видеоролик о правилах безопасности в интернете.

Практическая работа №. 3. Составить вопросы по теме "Угрозы и риски в сети Интернет" и провести викторину с одноклассниками.

Тема № 3. - 10ч

Безопасное поведение в Интернете

Основные вопросы: Что такое безопасное поведение в Интернете? Определение и значимость безопасного поведения. Основные принципы безопасности в цифровом пространстве. Какие риски существуют в Интернете? Обзор распространённых угроз: кибербуллинг, мошенничество, фишинг. Психологические аспекты интернет-травли и воздействия на пользователей. Как защитить свои личные данные? Значение конфиденциальности и последствия утечки личной информации. Подходы к установке надежных настроек конфиденциальности. Что такое кибербезопасность? Основные инструменты и технологии для обеспечения безопасности. Как реагировать на различные ситуации в интернете? Действия в случае кибератаки или утечки данных. Закладывание основ для создания безопасного цифрового окружения.

Требования к знаниям и умениям:

Обучающиеся должны понимать принципы безопасного поведения в Интернете. Способность идентифицировать угрозы и риски. Знание методов защиты личной информации и настройки конфиденциальности. Умение пользоваться инструментами для обеспечения безопасности. Осведомленность о своих правах как пользователя Интернета.

Тематика практических работ:

Практическая работа №. 1. Создание индивидуального плана по снижению времени, проводимого в интернете, включающий здоровье, учебу и другие сферы жизни.

Практическая работа №. 2. Использование мобильного приложения «МЧС России»

Практическая работа №. 1. Создание индивидуального плана по снижению времени, проводимого в интернете, включающий здоровье, учебу и другие сферы жизни.

Практическая работа №. 2. Использование мобильного приложения «МЧС России»

Тема № 4.- 10ч

Социальные сети и общение в сети

Основные вопросы: Каковы основные функции социальных сетей? Что такое социальные сети и их роль в современном обществе. Обзор популярных платформ (ВК, ТГ и др.). Как социальные сети влияют на общественные отношения? Позитивные и негативные аспекты (социальная связь, кибербуллинг). Влияние на психическое здоровье и самооценку. Как безопасно общаться в сети? Этикет и правила общения в социальных сетях. Как избежать конфликтов и недопонимания в онлайн-коммуникации. Как защитить свою личную информацию в социальных сетях? Настройки конфиденциальности и безопасности. Риски разглашения личных данных. Как распознавать и предотвращать кибербуллинг? Определение кибербуллинга и его последствия. Меры по предотвращению и реагированию на случаи кибербуллинга.

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 программы для общения, создание контактов. Отличать вредные игры от полезных.

Практическое занятие:

Практическая работа №. 1. Оцените уровень безопасности своих профилей и создайте план по его улучшению.

Практическая работа №. 2. Создание рекомендаций для безопасного общения в Интернете.

Практическая работа №.3 Настройка безопасного профиля и конфиденциальности в соц.сетях.

Тема №5. - 10ч

Киберзависимость и ее виды

Основные вопросы: Что такое киберзависимость? Определение киберзависимости и ее место в психологии. Признаки и симптомы. Виды киберзависимости: Зависимость от социальных сетей. Игровая зависимость. Зависимость от интернет-серфинга и просмотра контента. Зависимость от онлайн-коммуникаций (чаты, мессенджеры). Зависимость от онлайн-шопинга. Каковы причины киберзависимости? Психологические факторы (бегство от реальности, низкая самооценка). Социальные факторы (социальная изоляция, давление со стороны сверстников). Последствия киберзависимости: Влияние на психическое и физическое здоровье. Проблемы в учебе и работе. Угрозы личному и семейному благополучию. Методы преодоления киберзависимости: Определение временных рамок для

использования цифровой среды. Создание альтернативных хобби и активностей. Как защитить себя от информационной перегрузки.

Требования к знаниям и умениям: Понимание концепций и типов киберзависимости. Способность идентифицировать признаки киберзависимости у себя и окружающих. Осведомленность о возможных последствиях киберзависимости. Знание методов и стратегий борьбы с киберзависимостью. Умение информировать других о важности здорового использования технологий.

Практическое занятие:

Практическая работа №. 1. Тест «Есть у меня игровая зависимость».

Тема № 6. - 10ч

Интернет-продажи и Маркетплейсы

Основные вопросы: Как распознать надежные интернет-магазины и платформы? Средства проверки репутации магазинов (отзывы, рейтинги, наличие контактных данных). Какие виды интернет-мошенничества существуют? Обзор распространённых схем мошенничества (фишинг, подделка сайтов, мошеннические объявления). Политики возврата и обмена товара. Какие методы безопасности следует использовать при покупках? Рекомендации по использованию защищённых платёжных систем и карт. Важность надежных паролей и двухфакторной аутентификации. Как поступать в случае подозрительных ситуаций? Действия при получении подозрительного письма или звонка. Как сообщать о мошенничестве и защищать свои права. Роль информационной безопасности в онлайн-покупках. Каким сайтам при покупке можно доверять.

Требования к знаниям и умениям: Обучающиеся должны знать принципы работы интернет - магазинов, понятие «электронные деньги». Обучающиеся должны уметь дозированно использовать личную информацию в сети интернет. Уметь различать (распознавать) мошеннические действия.

Практическое занятие: 2

Практическая работа №. 1. Сравните наиболее безопасные платформы для интернет – покупок

Практическая работа №. 2. Онлайн квест на платформе Joyteka «Покупка в интернет-магазине».

Тема №7. - 5ч

Как уберечь себя и близких от мошенников

Основные вопросы: Что такое мошенничество и какие его виды существуют? Обзор основных схем мошенничества (фишинг, SMS-мошенничество, интернет-аферисты). Способы, которыми мошенники манипулируют жертвами. Как распознать мошеннические действия?

Признаки подозрительных звонков, сообщений и предложений. Как отличить реальные предложения от фальшивок. Как подготовить себя и близких к безопасному поведению? Обучение основам безопасности в интернете (защита личной информации и паролей). Создание привычки к проверке информации. Как действовать в случае подозрительных ситуаций? Порядок действий при получении подозрительного сообщения или звонка. Как сообщать о мошенничестве и куда обращаться за помощью. Что такое двухфакторная аутентификация.

Требования к знаниям и умениям: Понимание основ мошенничества и его различных форм. Умение распознавать подозрительные ситуации и правильно на них реагировать. Знание методов защиты личной информации и финансирования. Навыки работы с современными технологиями для обеспечения безопасности (например, установка программ защиты). Осведомлённость о правах потребителей и ресурсах для обращения за помощью.

Практическое занятие:

Практическая работа №. 1. Создание буклета или постера с основными рекомендациями по безопасности в Интернете, которыми можно делиться в школе или сообществе.

Практическая работа №.2. Подготовка алгоритма безопасного поведения, при звонках и СМС от мошенников.

УСЛОВИЯ РЕАЛИЗАЦИИ ПРОГРАММЫ

Акустические колонки. Документ-камера. Интерактивная доска. Классная доска. Компьютер (ноутбук). Многофункциональный центр (принтер, сканер, ксерокс). Мультимедийный проектор.

№ п/п	Тема	Планируемая дата проведения	Фактическая дата проведения	Примечание
	Тема № 1. - 15ч Интернет. Введение в информационную безопасность			
1	Что такое компьютер? Устройство компьютера.			
2	Глобальная информационная система сети «Интернет». Выход в Интернет.			
3	Практическая работа №. 1. Провести SWOT-анализ сети интернет.			
4	Что такое информационная безопасность?			
5	Основные термины и концепции.			
6	Последствия нарушений			

	информационной безопасности.			
7	Роль информационной безопасности в повседневной жизни.			
8	Обязанности пользователей.			
9	Технологии и инструменты защиты информации.			
10	Безопасность мобильных приложений			
11	Анализ угроз в интернете			
12	Роль информационной безопасности в повседневной жизни.			
13	Как выбирать безопасные сайты			
14	Важность информационной безопасности для людей			
15	Практическая работа №. 2. Разработайте рекомендации по созданию надёжных паролей.			
	Тема № 2. - 10ч Угрозы и риски в сети Интернет			
1	Что такое угрозы в сети Интернет?			
2	Определение и классификация угроз.			
3	Основные виды угроз в цифровом пространстве			
4	Практическая работа №. 2. Создать короткий видеоролик о правилах безопасности в интернете.			
5	Определение термина «риск» в контексте информационной безопасности.			
6	Как минимизировать угрозы и риски?			
7	Практическая работа №. 3. Составить вопросы по теме "Угрозы и риски в сети Интернет" и провести викторину с одноклассниками.			
8	Роль пользовательского поведения в снижении рисков.			
9	Законодательство и защита пользователей			
10	Практическая работа №. 1. Изучение маркеров фишингового письма и поиск различий между настоящим письмом и фальшивым.			
	Тема № 3. - 10ч Безопасное поведение в Интернете			
1	Что такое безопасное поведение в Интернете?			
2	Основные принципы безопасности в цифровом пространстве.			
3	Как защитить свои личные данные?			
4	Значение конфиденциальности и			

	последствия утечки личной информации.			
5	Практическая работа №. 1. Создание индивидуального плана по снижению времени, проводимого в интернете, включающий здоровье, учебу и другие сферы жизни.			
6	Какие риски существуют в Интернете?			
7	Психологическая безопасность в интернете			
8	Как реагировать на различные ситуации в интернете?			
9	Практическая работа №. 2. Использование мобильного приложения «МЧС России»			
10	Основные инструменты и технологии для обеспечения безопасности.			
	Тема № 4.- 10ч Социальные сети и общение в сети			
1	Каковы основные функции социальных сетей?			
2	Как правильно общаться с незнакомцами			
3	Практическая работа №. 1. Оцените уровень безопасности своих профилей и создайте план по его улучшению.			
4	Позитивные и негативные аспекты (социальная связь, кибербуллинг).			
5	Этикет и правила общения в социальных сетях.			
6	Что такое социальные сети и их роль в современном обществе.			
7	Практическая работа №. 2. Создание рекомендаций для безопасного общения в Интернете.			
8	Как избежать конфликтов и недопонимания в онлайн-коммуникации.			
9	Как безопасно общаться в сети?			
10	Практическая работа №.3 Настройка безопасного профиля и конфиденциальности в соц.сетях.			
	Тема №5. - 10ч Киберзависимость и ее виды			
1	Что такое киберзависимость?			

2	Тест «Есть у меня игровая зависимость».			
3	Определение киберзависимости и ее место в психологии.			
4	Признаки и симптомы.			
5	Виды киберзависимости.			
6	Зависимость от социальных сетей			
7	Игровая зависимость.			
8	Каковы причины киберзависимости?			
9	Последствия киберзависимости			
10	Методы преодоления киберзависимости			
	Тема № 6. - 10ч Интернет-продажи и Маркетплейсы			
1	Как распознать надежные интернет-магазины и платформы?			
2	Практическая работа №. 1. Сравните наиболее безопасные платформы для интернет – покупок			
3	Какие виды интернет-мошенничества существуют?			
4	Обзор распространённых схем мошенничества (фишинг, подделка сайтов, мошеннические объявления).			
5	Какие методы безопасности следует использовать при покупках?			
6	Практическая работа №. 2. Онлайн квест на платформе Joyteka «Покупка в интернет-магазине».			
7	Действия при получении подозрительного письма или звонка.			
8	Каким сайтам при покупке можно доверять.			
9	Политики возврата и обмена товара.			
10	Важность надежных паролей и двухфакторной аутентификации.			
	Тема №7. - 5ч Как уберечь себя и близких от мошенников			
1	Что такое мошенничество и какие его виды существуют?			
2	Как действовать в случае подозрительных ситуаций?			
3	Практическая работа №. 1. Создание буклета или постера с основными рекомендациями по безопасности в Интернете, которыми можно делиться в школе или сообществе.			
4	Как сообщать о мошенничестве и			

	куда обращаться за помощью.			
5	Практическая работа №.2. Подготовка алгоритма безопасного поведения, при звонках и СМС от мошенников.			

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. 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 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 программам 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. Колесниченко Денис. Анонимность и безопасность в интернете. От чайника к пользователю. Самоучитель Издательство: БХВ-Петербург, 2012, 240с.

2. Мазаник Сергей. Безопасность компьютера. Защита от сбоев, вирусов и неисправностей: издательство: ЭКСМО, 2014, 256 с.

3. Мэйволд Э. Безопасность сетей (2-е изд.) Книги» Сетевые Технологии. Название: Безопасностьсетей: Издательство: М.: НОУ "Интуит", 2016, 571 с.

4. Платонов В.В. Программно- аппаратные средства защиты информации: учебник для студ. Учрежд. высш. проф. образования / В. В. Платонов. — М.: Издательский центр «Академия», 2013, 336 с.

5. Проскурин В.Г. Защита в операционных системах: Издательство: Горячая линия-Телеком, 2014, 192 с.

6. Савченко Е. Кто, как и зачем следит за вами через интернет: Москва - Третий Рим, 2012, 100 с.

7. 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 Солдатов 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.

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>-