



МИНИСТЕРСТВО ПРОСВЕЩЕНИЯ РОССИЙСКОЙ ФЕДЕРАЦИИ
Министерство образования и науки Смоленской области
Администрация города Смоленска
МБОУ "СШ №17 им. Героя Российской Федерации А.Б. Буханова"

РАССМОТРЕНО
Руководитель
методического
объединения учителей
естественно-
математического цикла
 Базерова О.Г.
Протокол №1
от «30» августа 2024 г.

СОГЛАСОВАНО
Заместитель директора МБОУ
«СШ № 17 им. Героя
Российской Федерации А.Б.
Буханова»
 Силаева А.А.
«30» августа 2024 г.

УТВЕРЖДЕНО
Директор МБОУ "СШ№17 им.
Героя Российской Федерации
А.Б. Буханова»
Балыкина В.Д.
Приказ №65/14
от «30» августа 2024 г.



РАБОЧАЯ ПРОГРАММА
КУРСА ВНЕУРОЧНОЙ ДЕЯТЕЛЬНОСТИ
«ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ»

для обучающихся 10-11 классов

г. Смоленск 2024

I. Пояснительная записка

Развитие информационного общества предполагает внедрение информационных технологий во все сферы жизни, но это означает и появление новых угроз безопасности – от утечек информации до кибертерроризма. В проекте Концепции стратегии кибербезопасности Российской Федерации киберпространство определяется как «сфера деятельности в информационном пространстве, образованная совокупностью Интернета и других телекоммуникационных сетей и любых форм осуществляемой посредством их использования человеческой активности (личности, организации, государства)», а кибербезопасность – как «совокупность условий, при которых все составляющие киберпространства защищены от максимально возможного числа угроз и воздействий с нежелательными последствиями». В связи с этим большое значение приобретает проблема «культуры безопасного поведения в киберпространстве».

В соответствии со «Стратегией развития отрасли информационных технологий в Российской Федерации на 2014-2020 годы и на перспективу до 2025 года», утвержденной распоряжением Правительства Российской Федерации от 1 ноября 2013 г. № 2036-р, «Стратегией развития информационного общества в Российской Федерации», утвержденной Президентом Российской Федерации 7 февраля 2008 г. № Пр-212 и рядом других документов в числе многих других задач выделяются:

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

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

Киберугрозы существуют везде, где применяются информационные технологии, следовательно, любой человек может столкнуться и со спамом, и с вирусами, и со взломом компьютера и с многими другими проблемами, на которые нужно не только оперативно реагировать, но и насколько возможно уметь предотвращать их появление.

С учетом роста числа угроз информационной деятельности и стремительного развития информационных технологий представляется необходимым для каждого ученика знание «технических устройств (в том числе компьютеров)», умение «искать информацию с применением правил поиска (построения запросов) в базах данных, компьютерных сетях, пользоваться персональным компьютером и его периферийным оборудованием; следовать требованиям техники безопасности, гигиены, эргономики и ресурсосбережения при работе со средствами информационных и коммуникационных технологий», знание основ информационной безопасности, умения соблюдать требования информационной безопасности в практической деятельности и организовывать безопасность личного информационного пространства.

Цель изучения курса внеурочной деятельности «Информационная безопасность»:

дать общие представления о безопасности в информационном обществе и на этой основе сформировать понимание технологий информационной безопасности и умения применять правила информационной безопасности во всех сферах деятельности.

Задачи курса внеурочной деятельности «Информационная безопасность»

- совершенствование подготовки учащихся в сфере информационных технологий,
- популяризация профессий, связанных с информационными технологиями.

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

Курс внеурочной деятельности «Информационная безопасность» рассчитан на учащихся 10-11 классов.

II. Личностные, метапредметные и предметные результаты освоения курса внеурочной деятельности «Информационная безопасность»

Сформулированные цели реализуются через достижение образовательных результатов. Эти результаты структурированы по ключевым задачам общего образования, отражающим индивидуальные, общественные и государственные потребности, и включают в себя предметные, метапредметные и личностные результаты. Особенность курса заключается в том, что многие знания и способы деятельности (включая использование средств ИКТ) имеют значимость для разных предметных областей и формируются при их изучении.

Личностные результаты:

- формирование к саморазвитию и самообразованию на основе мотивации к ответственному отношению к учению, готовности и способности обучающихся обучению и познанию;
- формирование целостного мировоззрения, соответствующего современному уровню развития науки и общественной практики;

- развитие осознанного и ответственного отношения к собственным поступкам;
- формирование коммуникативной компетентности в процессе образовательной, учебно-исследовательской, творческой и других видов деятельности.

В сфере развития познавательных универсальных учебных действий приоритетное внимание уделяется:

- практическому освоению обучающимися основ проектно-исследовательской деятельности;
- развитию стратегий смыслового чтения и работе с информацией;
- практическому освоению методов познания, используемых в различных областях знания и сферах культуры, соответствующего им инструментария и понятийного аппарата, регулярному обращению в учебном процессе к использованию общеучебных умений, знаково-символических средств, широкого спектра логических действий и операций.

При изучении внеурочного курса «Информационная безопасность» **обучающиеся усваивают** приобретенные ранее навыки работы с информацией и пополняют их. Они смогут работать с текстами, графикой, преобразовывать и интерпретировать содержащуюся в них информацию, в том числе:

- систематизировать, сопоставлять, анализировать, обобщать и интерпретировать информацию, содержащуюся в готовых информационных объектах;
- выделять главную и избыточную информацию, выполнять смысловое свертывание выделенных фактов, мыслей; представлять информацию в сжатой словесной форме и в наглядно-символической форме;

- заполнять и дополнять таблицы, схемы, тексты, изображения.

Обучающиеся **усовершенствуют** навык поиска информации в компьютерных и некомпьютерных источниках информации, приобретут навык формулирования запросов и опыт использования поисковых машин. Они **научатся** осуществлять поиск информации в Интернете, школьном информационном пространстве, базах данных и на персональном компьютере с использованием поисковых сервисов, строить поисковые запросы в зависимости от цели запроса и анализировать результаты поиска.

Обучающиеся **приобретут потребность** поиска дополнительной информации для решения учебных задач и самостоятельной познавательной деятельности; освоят эффективные приемы поиска, организации и хранения информации на персональном компьютере, в информационной среде учреждения и в Интернете; **приобретут первичные навыки** формирования и организации собственного информационного пространства.

Они **усовершенствуют умение** передавать информацию в устной форме, сопровождаемой аудиовизуальной поддержкой, и в письменной форме гипермедиа (т. е. сочетания текста, изображения, звука, ссылок между разными информационными компонентами).

Обучающиеся **смогут использовать** информацию для установления причинно-следственных связей и зависимостей, объяснений и доказательств фактов в различных учебных и практических ситуациях, ситуациях моделирования и проектирования.

Школьники **получат возможность** научиться строить умозаключения и принимать решения на основе самостоятельно полученной информации, а также освоить опыт критического отношения к получаемой информации на основе её сопоставления с информацией из других источников и с имеющимся жизненным опытом.

Учащиеся научатся:

- основам реализации проектно-исследовательской деятельности;
- проводить наблюдение и эксперимент под руководством учителя;
- осуществлять расширенный поиск информации с использованием ресурсов библиотек и Интернета;
- создавать и преобразовывать модели и схемы для решения задач;
- осуществлять выбор наиболее эффективных способов решения задач в зависимости от конкретных условий;
- давать определение понятиям;
- устанавливать причинно-следственные связи;
- осуществлять логическую операцию установления родовидовых отношений, ограничение понятия;
- обобщать понятия - осуществлять логическую операцию перехода от видовых признаков к родовому понятию, от понятия с меньшим объемом к понятию с большим объемом;
- осуществлять сравнение, сериацию и классификацию, самостоятельно выбирая основания и критерии для указанных логических операций;
- строить логическое рассуждение, включающее установление причинно-следственных связей; • объяснять явления, процессы, связи и отношения, выявляемые в ходе исследования;
- основам ознакомительного, изучающего, усваивающего и поискового чтения;

- структурировать тексты, включая умение выделять главное и второстепенное, главную идею текста, выстраивать последовательность описываемых событий;
- работать с метафорами - понимать переносный смысл выражений, понимать и употреблять обороты речи, построенные на скрытом уподоблении, образном сближении слов.

Обучающиеся получают возможность научиться:

- основам дизайна и web-дизайна;
- ставить проблему, аргументировать её актуальность;
- самостоятельно проводить исследование на основе применения методов наблюдения и эксперимента; • выдвигать гипотезы о связях и закономерностях событий, процессов, объектов;
- организовывать исследование с целью проверки гипотез;
- делать умозаключения (индуктивное и по аналогии) и выводы на основе аргументации.

Формирование ИКТ-компетентности обучающихся. Учащиеся научатся:

- подключать устройства ИКТ к электрическим и информационным сетям, использовать аккумуляторы;
- соединять устройства ИКТ (блоки компьютера, устройства сетей, принтер, проектор, сканер, измерительные устройства и т. д.) с использованием проводных и беспроводных технологий;
- правильно включать и выключать устройства ИКТ, входить в операционную систему и завершать работу с ней, выполнять базовые действия с экранными объектами (перемещение курсора, выделение, прямое перемещение, запоминание и вырезание);

- осуществлять информационное подключение к локальной сети и глобальной сети Интернет;
 - входить в информационную среду образовательного учреждения, в том числе через Интернет, размещать в информационной среде различные информационные объекты;
 - выводить информацию на бумагу, правильно обращаться с расходными материалами;
 - соблюдать требования техники безопасности, гигиены, эргономики и ресурсосбережения при работе с устройствами ИКТ, в частности учитывающие специфику работы с различными экранами;
- осуществлять фиксацию изображений и звуков в ходе процесса обсуждения, проведения эксперимента, природного процесса, фиксацию хода и результатов проектной деятельности;
- учитывать смысл и содержание деятельности при организации фиксации, выделять для фиксации отдельные элементы объектов и процессов, обеспечивать качество фиксации существенных элементов;
 - выбирать технические средства ИКТ для фиксации изображений и звуков в соответствии с поставленной целью;
 - проводить обработку цифровых фотографий с использованием возможностей специальных компьютерных инструментов, создавать презентации на основе цифровых фотографий;
 - проводить обработку цифровых звукозаписей с использованием возможностей специальных компьютерных инструментов, проводить транскрибирование цифровых звукозаписей;
 - осуществлять видеосъемку и проводить монтаж отснятого материала с использованием возможностей специальных компьютерных инструментов;

организовывать сообщения в виде линейного или включающего ссылки представления для самостоятельного просмотра через браузер;

- работать с особыми видами сообщений: диаграммами (алгоритмические, концептуальные, классификационные, организационные, родства и др.), картами (географические, хронологические) и спутниковыми фотографиями, в том числе в системах глобального позиционирования;

- проводить деконструкцию сообщений, выделение в них структуры, элементов и фрагментов; • использовать при восприятии сообщений внутренние и внешние ссылки;

- формулировать вопросы к сообщению, создавать краткое описание сообщения; цитировать фрагменты сообщения;

- избирательно относиться к информации в окружающем информационном пространстве, отказываться от потребления ненужной информации;

создавать различные геометрические объекты с использованием возможностей специальных компьютерных инструментов;

- создавать цифровые продукты с использованием специализированных компьютерных программ. Учащиеся получают возможность научиться:

- осознавать и использовать в практической деятельности основные психологические особенности восприятия информации человеком;

- различать творческую и техническую фиксацию звуков и изображений;

- использовать возможности ИКТ в творческой деятельности, связанной с искусством. • создавать мультипликационные фильмы.

Коммуникация и социальное взаимодействие Учащиеся научатся:

- осуществлять образовательное взаимодействие в информационном пространстве образовательного учреждения (получение и выполнение

заданий, получение комментариев, совершенствование своей работы, формирование портфолио);

- соблюдать нормы информационной культуры, этики и права; с уважением относиться к частной информации и информационным правам других людей.
- формировать собственное информационное пространство: создавать системы папок и размещать в них нужные информационные источники, размещать информацию в Интернете.
- проектировать и организовывать свою индивидуальную и групповую деятельность, организовывать свое время с использованием ИКТ.

Учащиеся получают возможность научиться:

- взаимодействовать с партнерами с использованием возможностей Интернета (игровое и театральное взаимодействие).

Метапредметные результаты:

1. умение самостоятельно определять цели своего обучения, ставить и формулировать для себя новые задачи в учебе и познавательной деятельности, развивать мотивы и интересы своей познавательной деятельности;
2. владение основами самоконтроля, самооценки, принятия решений и осуществления осознанного выбора в учебной и познавательной деятельности;
3. умение определять понятия, создавать обобщения, устанавливать аналогии, классифицировать, самостоятельно выбирать основания и критерии для классификации, устанавливать причинно-следственные связи, строить логическое рассуждение, умозаключение (индуктивное, дедуктивное и по аналогии) и делать выводы;
4. умение создавать, применять и преобразовывать знаки и символы, модели и схемы для решения учебных и познавательных задач;

5. смысловое чтение;
6. умение осознанно использовать речевые средства в соответствии с задачей коммуникации; владение устной и письменной речью;
7. формирование и развитие компетентности в области использования информационно-коммуникационных технологий (далее ИКТ-компетенции).

Предметные результаты:

1. умение использовать термины «информация», «сообщение», «данные», «графика», «алгоритм», «анимация», «программа», «дизайн», «web-сайт», «издательское дело»; понимание различий между употреблением этих терминов в быденной речи и в информатике;
2. умение описывать структуру сайта, используя основы языка HTML; умение создавать и редактировать растровые изображения;
3. умение создавать и редактировать векторные изображения; умение создавать flash-анимацию различными методами; умение создавать дизайн и верстку печатного издания;
4. умение использовать готовые прикладные компьютерные программы и сервисы в выбранной специализации, умение работать с описаниями программ и сервисами;
5. навыки выбора способа представления данных в зависимости от поставленной задачи.

III. Содержание курса внеурочной деятельности «Информационная безопасность»

10 класс

Техника безопасности и экология

1. Компьютер и мобильные (сотовые) устройства в правилах безопасности
2. Компьютеры и мобильные устройства в экстремальных условиях
3. Везде ли есть Интернет. ТБ при работе с мобильными устройствами 18
4. Первая помощь при проблемах в интернете (службы помощи)
5. Компьютер и зрение
6. Воздействие радиоволн на здоровье и окружающую среду (Wi-Fi, Bluetooth, GSM)
7. Проблемы Интернет-зависимости
8. Виды Интернет-зависимости

Общие сведения о безопасности ПК и Интернета

1. Как работают мобильные устройства. Угрозы для мобильных устройств
2. Распространение вредоносных файлов через приложения для смартфонов и планшетов (скачивание фотографий, музыки, игр)
3. Виды защиты киберпространства (что такое несанкционированный доступ, разрушение и утрата информации, искажение информации)
4. Кто обеспечивает защиту киберпространства
5. Что такое геоинформационные системы. Глобальные информационные Сети по стихийным бедствиям

Методы обеспечения безопасности ПК и Интернета. Вирусы и антивирусы

1. Как распространяются вирусы
2. Источники и причины заражения
3. Скорая компьютерная помощь. Признаки заражения компьютера
4. Что такое антивирусная защита. Как лечить компьютер
5. Защита мобильных устройств
6. Как защитить данные от потерь. Копирование и восстановление.
Всегда ли можно спасти свои данные
7. Защита файлов. Что такое право доступа
8. Защита детей в социальных сетях. ПО для родителей. Ограничение времени нахождения в сети

Мошеннические действия в Интернете. Киберпреступления

1. Опасности мобильной связи. Предложения по установке вредоносных приложений. Мошеннические СМС
2. Прослушивание разговоров. Определение местоположения телефона

Сетевой этикет. Психология и сеть

1. Что такое личные данные. Все, что выложено в Интернет, может стать известно всем
2. «Лишняя информация» о себе и других в Интернете. Какая информация принадлежит вам
3. Анонимность в сети
4. Что такое этикет. Виды этикета (личный, деловой, письменный, дискуссионный и пр.). Различия этикета в разных странах
5. Как появился нетикет, что это такое. Общие правила сетевого этикета
6. Личное общение и общение в группе – чем они отличаются (чаты, форумы, службы мгновенных сообщений)

7. Этика дискуссий. Взаимное уважение при интернет-общении
8. Этикет и безопасность. Эмоции в сети, их выражение
9. Реальная и виртуальная личность, реальные встречи с виртуальными знакомыми и их опасность, угрозы и оскорбления – чем это может закончиться
10. Психологическая обстановка в Интернете: гриффинг, кибербуллинг, кибермоббинг, троллинг, буллицид
11. Если вы стали жертвой компьютерной агрессии: службы помощи

Правовые аспекты защиты киберпространства

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

11 класс

Общие сведения о безопасности ПК и Интернета

1. Информационная безопасность
2. Защита персональных данных, почему она нужна. Категории персональных данных. Биометрические персональные данные
3. Источники данных в Интернете: почта, сервисы обмена файлами и др.
4. Хранение данных в Интернете
5. Возможности и проблемы социальных сетей
6. Безопасный профиль в социальных сетях. Составление сети контактов

Техника безопасности и экология

1. Комплекс упражнений при работе за компьютером
2. Воздействие на зрение ЭЛТ, жидкокристаллических, светодиодных, монохромных мониторов

Проблемы Интернет-зависимости

1. Для чего может быть полезен ПК и Интернет (развивающие игры, обучение, общение и т.п.) и как польза превращается во вред
2. Киберкультура (массовая культура в сети) и личность
3. Психологическое воздействие информации на человека. Управление личностью через сеть

Методы обеспечения безопасности ПК и Интернета. Вирусы и антивирусы

1. Защита файлов. Права пользователей

2. Защита при загрузке и выключении компьютера
3. Безопасность при скачивании файлов
4. Безопасность при просмотре фильмов онлайн
5. Защита программ и данных от несанкционированного копирования. Организационные, юридические, программные и программно-аппаратные меры защиты
6. Защита программ и данных с помощью паролей, программных и электронных ключей, серийных номеров, переноса в онлайн и т.п. Неперемещаемые программы.
7. Методы защиты фото и видеоматериалов от копирования в сети
8. Защита от копирования контента сайта
9. Как развивались вирусы
10. Могут ли вирусы воздействовать на аппаратуру ПК
11. Как вирусы воздействуют на файлы
12. Проверка на наличие вирусов. Сканеры и др.
13. Может ли вирус воздействовать на рабочий стол
14. Источники заражения ПК
15. Антивирусное ПО, виды и назначение
16. Методы защиты от вирусов. Как распознаются вирусы

Мошеннические действия в Интернете. Киберпреступления

1. Утечка и обнародование личных данных
2. Подбор и перехват паролей. Взломы аккаунтов в социальных сетях
3. Виды мошенничества в Интернете. Фишинг (фарминг)
4. Азартные игры. Онлайн-казино. Букмекерские конторы. Предложения для «инвестирования» денег. Выигрыш в лотерею

Правовые аспекты защиты киберпространства

1. Защита прав потребителей при использовании услуг Интернет
2. Защита прав потребителей услуг провайдера

IV. Описание учебно-методического и материально-технического обеспечения курса внеурочной деятельности

Литература:

1. Бирюков А.А. Информационная безопасность защита и нападение 2-е издание Издательство: ДМК-Пресс., 2017, 434 с.
2. Колесниченко Денис. Анонимность и безопасность в интернете. От чайника к пользователю. Самоучитель Издательство: БХВ-Петербург, 2012, 240с.
3. Мазаник Сергей. Безопасность компьютера. Защита от сбоев, вирусов и неисправностей: издательство: ЭКСМО, 2014, 256 с.
4. Мэйволд Э. Безопасность сетей (2-е изд.) Книги» Сетевые Технологии. Название: Безопасностьсетей: Издательство: М.: НОУ "Интуит", 2016,571 с.
5. 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.
6. Проскурин В.Г Защита в операционных системах: Издательство: Горячая линия-Телеком, 2014, 192 с.
7. Савченко Е. Кто, как и зачем следит за вами через интернет: Москва - Третий Рим, 2012, 100 с.
8. Яковлев В.А. Шпионские и антишпионские штучки: Техническая литература Издательство: Наука и Техника, 2015, 320 с.
9. "Березовый лес" или "лес березовый" /П. Лауфер//Юный эрудит. - 2014. - № 3. - С. 24-26
10. Доценко С.М., Шпак В.Ф. Комплексная информационная безопасность объекта. От теории к практике, Издательство: ООО «Издательство Полигон», 2000, 215 с.

11. Клепа и железный друг//Клепа. - 2014. - № 8. - С. 1-33.Электронная версия журнала: <http://klepa.ru>.
12. Методическое пособие для работников системы общего образования Солдатов Г., Зотова Е., Лебешева М., Шляпников В. «Интернет: возможности, компетенции, безопасность», 2015 - 156с.
13. 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.:
14. 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) http://nto.immpu.sgu.ru/sites/default/files/3/_12697.pdf -Рыжков В.Н. методика преподавания информатики;
- 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 Интернете"

12) <http://www.ifap.ru> — интерактивный курс по Интернет-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;

Полезные ссылки для обучающихся:

1) http://www.symantec.com/ru/ru/norton/clubsymantec/library/article.jsp?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=bdnXmTpZX04&feature=related>
3. Линия помощи "Дети онлайн"
<http://www.youtube.com/watch?v=qivz1wJoxk4>
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

Материальная база кабинета:

- компьютеры;
- проектор;
- экран;
- колонки;
- принтер.

VI. Календарно – тематическое планирование по курсу внеурочной деятельности «Информационная безопасность»

(10 класс)

№ п/п	Тема урока	кол-во часов	Дата проведения	Дата изменения
Общие сведения о безопасности ПК и Интернета				
1	Как работают мобильные устройства. Угрозы для мобильных устройств	1		
2	Распространение вредоносных файлов через приложения для смартфонов и планшетов (скачивание фотографий, музыки, игр)	1		
3	Виды защиты киберпространства (что такое несанкционированный доступ, разрушение и утрата информации, искажение информации)	1		
4	Кто обеспечивает защиту киберпространства	1		
5	Что такое геоинформационные системы. Глобальные информационные Сети по стихийным бедствиям	1		
Техника безопасности и экология				
6	Дополнения к ДТП. Компьютер и мобильные (сотовые) устройства в правилах безопасности	1		
7	Компьютеры и мобильные устройства в экстремальных условиях	1		
8	Везде ли есть Интернет. ТБ при работе с мобильными устройствами 18	1		
9	Первая помощь при проблемах в интернете (службы помощи)	1		
10	Компьютер и зрение	1		
11	Воздействие радиоволн на здоровье и окружающую среду (Wi-Fi, Bluetooth, GSM)	1		
12	Проблемы Интернет-зависимости	1		
13	Виды Интернет-зависимости	1		
Методы обеспечения безопасности ПК и Интернета. Вирусы и антивирусы				
14	Как распространяются вирусы	1		
15	Источники и причины заражения	1		
16	Скорая компьютерная помощь. Признаки заражения компьютера	1		
17	Что такое антивирусная защита. Как лечить компьютер	1		
18	Защита мобильных устройств	1		

19	Как защитить данные от потерь. Копирование и восстановление. Всегда ли можно спасти свои данные	1		
20	Защита файлов. Что такое право доступа	1		
21	Защита детей в социальных сетях. ПО для родителей. Ограничение времени нахождения в сети	1		
Мошеннические действия в Интернете. Киберпреступления				
22	Опасности мобильной связи. Предложения по установке вредоносных приложений. Мошеннические СМС	1		
23	Прослушивание разговоров. Определение местоположения телефона	1		
Сетевой этикет. Психология и сеть				
24	Интернет, может стать известно всем	1		
25	«Лишняя информация» о себе и других в Интернете. Какая информация принадлежит вам	1		
26	Анонимность в сети	1		
27	Что такое этикет. Виды этикета (личный, деловой, письменный, дискуссионный и пр.). Различия этикета в разных странах	1		
28	Как появился нетикет, что это такое. Общие правила сетевого этикета	1		
29	Личное общение и общение в группе – чем они отличаются (чаты, форумы, службы мгновенных сообщений)	1		
30	Этика дискуссий. Взаимное уважение при интернет-общении	1		
31	Этикет и безопасность. Эмоции в сети, их выражение	1		
32	Реальная и виртуальная личность, реальные встречи с виртуальными знакомыми и их опасность, угрозы и оскорбления – чем это может закончиться	1		
33	Психологическая обстановка в Интернете: гриффинг, кибербуллинг, кибермоббинг, троллинг, буллицид	1		
34	Если вы стали жертвой компьютерной агрессии: службы помощи	1		

(11 класс)

№ п/п	Тема урока	кол-во часов	Дата проведения	Дата изменения
Техника безопасности и экология				
1	Комплекс упражнений при работе за компьютером	2		
2	Воздействие на зрение ЭЛТ, жидкокристаллических, светодиодных, монохромных мониторов	2		
Общие сведения о безопасности ПК и Интернета				
3	Информационная безопасность	2		
4	Защита персональных данных, почему она нужна. Категории персональных данных. Биометрические персональные данные	2		
5	Источники данных в Интернете: почта, сервисы обмена файлами и др.	2		
6	Хранение данных в Интернете	2		
7	Возможности и проблемы социальных сетей	2		
8	Безопасный профиль в социальных сетях. Составление сети контактов	2		
Проблемы Интернет-зависимости				
9	Для чего может быть полезен ПК и Интернет (развивающие игры, обучение, общение и т.п.) и как польза превращается во вред	2		
10	Киберкультура (массовая культура в сети) и личность	2		
11	Психологическое воздействие информации на человека. Управление личностью через сеть	2		
Методы обеспечения безопасности ПК и Интернета.				
Вирусы и антивирусы				
12	Защита файлов. Права пользователей	2		
13	Защита при загрузке и выключении компьютера	2		
14	Безопасность при скачивании файлов	2		
15	Безопасность при просмотре фильмов онлайн	2		
16	Защита программ и данных от несанкционированного копирования. Организационные, юридические, программные и программно-аппаратные меры защиты	2		
17	Защита программ и данных с помощью паролей, программных и электронных ключей, серийных	2		

	номеров, переноса в онлайн и т.п. Неперемещаемые программы.			
18	Методы защиты фото и видеоматериалов от копирования в сети	2		
19	Защита от копирования контента сайта	2		
20	Как развивались вирусы	2		
21	Могут ли вирусы воздействовать на аппаратуру ПК	2		
22	Как вирусы воздействуют на файлы	2		
23	Проверка на наличие вирусов. Сканеры и др.	2		
24	Может ли вирус воздействовать на рабочий стол	2		
25	Источники заражения ПК	2		
26	Антивирусное ПО, виды и назначение	2		
27	Методы защиты от вирусов. Как распознаются вирусы	2		
Мошеннические действия в Интернете.				
Киберпреступления				
28	Утечка и обнародование личных данных	2		
29	Подбор и перехват паролей. Взломы аккаунтов в социальных сетях	2		
30	Виды мошенничества в Интернете. Фишинг (фарминг)	2		
31	Азартные игры. Онлайн-казино. Букмекерские конторы. Предложения для «инвестирования» денег. Выигрыш в лотерею	2		
Правовые аспекты защиты киберпространства				
32	Защита прав потребителей при использовании услуг Интернет	2		
33	Защита прав потребителей услуг провайдера	2		