Государственное бюджетное общеобразовательное учреждение Самарской области средняя общеобразовательная школа «Образовательный центр» с. Александровка муниципального района Кинель — Черкасский Самарской области

446327 Самарская область, Кинель-Черкасский район, с. Александровка, ул. Школьная, д. 14

Телефон (факс) 8 (84660) 3 – 35 – 18, электронный адрес: alex_sch@samara.edu

Подписан: Егорова Надежда Анатольевна
DN: C=RU, OU=Директор школы, O="ГБОУ СОШ ""Оц"" с. Александровка м.р.Кинель-Черкасский", CN=Егорова Надежда Анатольевна, E=alex_sch@samara.edu.ru
Основание: я подтверждаю этот документ своей удостоверяющей подписью
Местоположение: место подписания
Дата: 2021-08-30 10:35:51
Foxit Reader Версия: 9.7.2

РАБОЧАЯ ПРОГРАММА

КУРСА ВНЕУРОЧНОЙ ДЕЯТЕЛЬНОСТИ

«ЦИФРОВАЯ ГИГИЕНА»

Уровень образования **основное общее**

Составитель (составители) **Кондрашова Н.Д**

«СОГЛАСОВАНО»
Заместитель директора по ВР:
_____Кондрашова Н.Д.
Дата: 30.08.2021 г.

«СОГЛАСОВАНО НА ЗАСЕДАНИИ МО»
Протокол №1 от 27.08.2021 г.
Председатель МО:
_____ Милёшина И.В.

Пояснительная записка

Программа курса «Цифровая гигиена» составлена на основе: Примерная рабочая программа учебного курс «Цифровая гигиена», рекомендованная Координационным советом учебно-методических объединений в системе общего образования Самарской области.

Данная программа адресована учащимся 5-9 классов и учитывает требования, выдвигаемые федеральным государственным образовательным стандартом основного общего образования к предметным (образовательные области «Математика и информатика», «Физическая культура и основы безопасности жизнедеятельности»), метапредметным и личностным результатам.

Основными целями изучения курса «Цифровая гигиена» являются:

 обеспечение условий для профилактики негативных тенденций в информационной культуре учащихся, повышения защищенности детей от информационных рисков и угроз;

 формирование навыков своевременного распознавания онлайн-рисков (технического, контентного, коммуникационного, потребительского характера и риска интернет-зависимости).

Задачи программы:

 сформировать общекультурные навыки работы с информацией (умения, связанные с поиском, пониманием, организацией, архивированием цифровой информации и ее критическим осмыслением, а также с созданием информационных объектов с использованием цифровых ресурсов (текстовых, изобразительных, аудио и видео);

 создать условия для формирования умений, необходимых для различных форм коммуникации (электронная почта, чаты, блоги, форумы, социальные сети и др.) с различными целями и ответственного отношения к взаимодействию в современной информационно-телекоммуникационной среде;

 сформировать знания, позволяющие эффективно и безопасно использовать технические и программные средства для решения различных задач, в том числе использования компьютерных сетей, облачных сервисов и т.п.;

 сформировать знания, умения, мотивацию и ответственность, позволяющие решать с помощью цифровых устройств и интернета различные повседневные задачи, связанные с конкретными жизненными ситуациями, предполагающими удовлетворение различных потребностей;

 сформировать навыки по профилактике и коррекции зависимого поведения школьников, связанного с компьютерными технологиями и Интернетом.

Общая характеристика учебного курса

Курс «Цифровая гигиена» является важной составляющей работы с обучающимися, активно использующими различные сетевые формы общения (социальные сети, игры, пр.) с целью мотивации ответственного отношения к

обеспечению своей личной безопасности, безопасности своей семьи и своих друзей. Кроме того, реализация курса создаст условия для сокращения цифрового разрыва между поколениями и позволит родителям выступать в качестве экспертов, передающих опыт.

Данный курс предполагает организацию работы в соответствии с содержанием 1-ого модуля, предназначенного для обучающихся 5-9 классов.

Модуль 1. «Информационная безопасность»

Отбор тематики содержания курса осуществлен с учетом целей и задач ФГОС основного общего образования, возрастных особенностей и познавательных возможностей обучающихся 5-9 классов. Рекомендуется для реализации в рамках внеурочной деятельности обучающихся.

Для преподавании модуля «Информационная безопасность» могут использоваться разнообразные форматы обучения:

 традиционный урок (коллективная и групповая формы работы);

 тренинги (в классической форме или по кейс-методу);

 дистанционное обучение (электронные курсы, видеоролики, почтовые рассылки, микрообучение);

 смешанный формат.

Система учебных заданий должна создавать условия для формирования активной позиции школьников в получении знаний и умений выявлять информационную угрозу, определять степень ее опасности, предвидеть последствия информационной угрозы и противостоять им и профилактики негативных тенденций в развитии информационной культуры учащихся, повышения защищенности детей от информационных рисков и угроз (составление памяток, анализ защищенности собственных аккаунтов в социальных сетях и электронных сервисах, практические работы и т.д.).

Характеристика личностных, метапредметных и предметных результатов освоения учебного курса (Модуль 1)

Предметные:

Выпускник научится:

 анализировать доменные имена компьютеров и адреса документов в интер-нете;

 безопасно использовать средства коммуникации,

 безопасно вести и применять способы самозащиты при попытке мошенничества,

 безопасно использовать ресурсы интернета.

Выпускник овладеет:

 приемами безопасной организации своего личного пространства данных с использованием индивидуальных накопителей данных, интернет-сервисов и т.п.

Выпускник получит возможность овладеть:

 основами соблюдения норм информационной этики и права;

 основами самоконтроля, самооценки, принятия решений и осуществления осознанного выбора в учебной и познавательной деятельности при формировании современной культуры безопасности жизнедеятельности;

 использовать для решения коммуникативных задач в области безопасности жизнедеятельности различные источники информации, включая Интернет-ресурсы и другие базы данных.

Метапредметные.

Регулятивные универсальные учебные действия.

В результате освоения учебного курса обучающийся сможет:

 идентифицировать собственные проблемы и определять главную проблему;

 выдвигать версии решения проблемы, формулировать гипотезы, предвосхищать конечный результат;

 ставить цель деятельности на основе определенной проблемы и существующих возможностей;

 выбирать из предложенных вариантов и самостоятельно искать средства/ресурсы для решения задачи/достижения цели;

 составлять план решения проблемы (выполнения проекта, проведения исследования);

 описывать свой опыт, оформляя его для передачи другим людям в виде технологии решения практических задач определенного класса;

 оценивать свою деятельность, аргументируя причины достижения или отсутствия планируемого результата;

 находить достаточные средства для выполнения учебных действий в изменяющейся ситуации и/или при отсутствии планируемого результата;

 работая по своему плану, вносить коррективы в текущую деятельность на основе анализа изменений ситуации для получения запланированных характеристик продукта/результата;

 принимать решение в учебной ситуации и нести за него ответственность.

Познавательные универсальные учебные действия.
В результате освоения учебного курса обучающийся сможет:
 выделять явление из общего ряда других явлений;
 определять обстоятельства, которые предшествовали возникновению связи между явлениями, из этих обстоятельств выделять определяющие, способные быть причиной данного явления, выявлять причины и следствия явлений;
 строить рассуждение от общих закономерностей к частным явлениям и от частных явлений к общим закономерностям;
 излагать полученную информацию, интерпретируя ее в контексте решаемой задачи;
 самостоятельно указывать на информацию, нуждающуюся в проверке, предлагать и применять способ проверки достоверности информации;
 критически оценивать содержание и форму текста;
 определять необходимые ключевые поисковые слова и запросы.

Коммуникативные универсальные учебные действия.
В результате освоения учебного курса обучающийся сможет:
 строить позитивные отношения в процессе учебной и познавательной деятельности;
 критически относиться к собственному мнению, с достоинством признавать ошибочность своего мнения (если оно таково) и корректировать его;
 договариваться о правилах и вопросах для обсуждения в соответствии с поставленной перед группой задачей;
 делать оценочный вывод о достижении цели коммуникации непосредственно после завершения коммуникативного контакта и обосновывать его.
 целенаправленно искать и использовать информационные ресурсы, необходимые для решения учебных и практических задач с помощью средств ИКТ;
 выбирать, строить и использовать адекватную информационную модель для передачи своих мыслей средствами естественных и формальных языков в соответствии с условиями коммуникации;
 использовать компьютерные технологии (включая выбор адекватных задаче инструментальных программно-аппаратных средств и сервисов) для
решения информационных и коммуникационных учебных задач, в том числе: вычисление, написание писем, сочинений, докладов, рефератов, создание презентаций и др.;
 использовать информацию с учетом этических и правовых норм;
 создавать информационные ресурсы разного типа и для разных аудиторий, соблюдать информационную гигиену и правила информационной безопасности.

Личностные.
 осознанное, уважительное и доброжелательное отношение к окружающим людям в реальном и виртуальном мире, их позициям, взглядам, готовность вести диалог с другими людьми, обоснованно осуществлять выбор виртуальных собеседников;
 готовность и способность к осознанному выбору и построению дальнейшей индивидуальной траектории образования на базе ориентировки в мире профессий и профессиональных предпочтений, с учетом устойчивых познавательных интересов;
 освоенность социальных норм, правил поведения, ролей и форм социальной жизни в группах и сообществах;
 сформированность понимания ценности безопасного образа жизни; интериоризация правил индивидуального и коллективного безопасного поведения в информационно-телекоммуникационной среде.

Воспитательные.

Результаты первого уровня (приобретение социальных знаний, понимания социальной реальности и повседневной жизни):

 приобретение знаний

- об этике и эстетике повседневной жизни человека в обществе;
- о принятых в обществе нормах поведения и общения;
- об основах здорового образа жизни;
- о правилах конструктивной групповой работы;
- об основах разработки социальных проектов и организации коллективной творческой деятельности;
- о способах самостоятельного поиска, нахождения и обработки информации;
- о правилах проведения исследования.

Формы достижения результатов первого уровня: познавательные беседы, инструктажи, социальные пробы, беседы о здоровом образе жизни.

Формы контроля результатов первого уровня: анкетирование.

Результаты второго уровня (получение опыта переживания и позитивного отношения к базовым ценностям общества):

- развитие ценностного отношения подростков к труду, знаниям, своему собственному здоровью и внутреннему миру;
- получение первоначального опыта самореализации.

Формы достижения результатов второго уровня: социально-значимые акции в клубе и в школе.

Формы контроля результатов второго уровня: защита конечного продукта (презентация созданного документа).

Результаты третьего уровня (получение опыта самостоятельного общественного действия):

- приобретение опыта исследовательской деятельности;
- опыт публичного выступления;
- опыт самообслуживания, самоорганизации и организации совместной деятельности с другими детьми.

Формы достижения результатов третьего уровня: исследовательские работы, социально-значимые акции в социуме (вне ОУ).

Формы контроля результатов третьего уровня: исследовательские конференции, конкурсы авторских работ.

Содержание программы учебного курса (Модуль 1)

Содержание программы учебного курса (Модуль 1) соответствует темам *примерной основной образовательной программы основного общего образования (ПООП ООО) по учебным предметам «Информатика» и «Основы безопасности жизнедеятельности»*, а также расширяет их за счет привлечения жизненного опыта обучающихся в использовании всевозможных технических устройств (персональных компьютеров, планшетов, смартфонов и пр.), позволяет правильно ввести ребенка в цифровое пространство и корректировать его поведение в виртуальном мире.

Основное содержание программы представлено разделами «Безопасность общения», «Безопасность устройств», «Безопасность информации».

Каждый раздел учебного курса (Модуля 1) завершается выполнением проектной работы по одной из тем, предложенных на выбор учащихся и/или проверочного теста.

Эти занятия в качестве волонтерской практики могут быть проведены учащимися, освоившими программу. Для проведения занятий могут быть использованы презентации, проекты, памятки, онлайн занятия, подготовленные в ходе выполнения учебных заданий по основным темам курса.

Содержание учебного курса (Модуль 1)

5 класс (34 часа)

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

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 информационнаябезопасность, 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.

Практическая работа. Составить информационный буклет «Моя безопасная сеть» или сделать групповую газету «Безопасность в Интернет».

Техника безопасности и экология (5 часов).

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

Практическая работа. Создание буклета «Техника безопасности при работе с компьютером».

Проблемы Интернет-зависимости (5 часов).

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).

Практическая работа. «Создание мультимедийной презентации «ПК и ЗОЖ. Организация рабочего места».

Методы обеспечения безопасности ПК и Интернета. Вирусы и антивирусы. (6 часов).

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.

Практическая работа «Установка антивирусной программы»;

Практическая работа. Создание презентации на тему: «Разновидности вирусов Черви, трояны, скрипты», «Шпионские программы», «Шифровальщики». «Троян-вымогатель в социальной сети “ВКонтакте” или наказание для особо любопытных».

Мошеннические действия в Интернете. Киберпреступления. (5 часов).

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.

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

Сетевой этикет. Психология и сеть. (4 часа).

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).

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

Государственная политика в области кибербезопасности. (5 часов).

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.

Практическая работа «Буклет. Правовые основы для защиты от спама».

Практическая работа. Создание презентации «Как уберечь свою персональную информацию в Интернете, если вы общаетесь в социальных сетях».

6 класс (34 часа)

Раздел 1. «Безопасность общения»

Тема 1. Общение в социальных сетях и мессенджерах. 1 час.

Социальная сеть. История социальных сетей. Мессенджеры. Назначение социальных сетей и мессенджеров. Пользовательский контент.

Тема 2. С кем безопасно общаться в интернете. 1 час.

Персональные данные как основной капитал личного пространства в цифровом мире. Правила добавления друзей в социальных сетях. Профиль пользователя. Анонимные социальные сети.

Тема 3. Пароли для аккаунтов социальных сетей. 1 час.

Сложные пароли. Онлайн генераторы паролей. Правила хранения паролей. Использование функции браузера по запоминанию паролей.

Тема 4. Безопасный вход в аккаунты. 1 час.

Виды аутентификации. Настройки безопасности аккаунта. Работа на чужом компьютере с точки зрения безопасности личного аккаунта.

Тема 5. Настройки конфиденциальности в социальных сетях. 1 час.

Настройки приватности и конфиденциальности в разных социальных сетях. Приватность и конфиденциальность в мессенджерах.

Тема 6. Публикация информации в социальных сетях. 1 час.

Персональные данные. Публикация личной информации.

Тема 7. Кибербуллинг. 1 час.

Определение кибербуллинга. Возможные причины кибербуллинга и как его избежать? Как не стать жертвой кибербуллинга. Как помочь жертве кибербуллинга.

Тема 8. Публичные аккаунты. 1 час.

Настройки приватности публичных страниц. Правила ведения публичных страниц. Овершеринг.

Тема 9. Фишинг. 2 часа.

Фишинг как мошеннический прием. Популярные варианты распространения фишинга. Отличие настоящих и фишинговых сайтов. Как защититься от фишеров в социальных сетях и мессенджерах.

Выполнение и защита индивидуальных и групповых проектов. 3 часа.

Раздел 2. «Безопасность устройств»

Тема 1. Что такое вредоносный код. 1 час.

Виды вредоносных кодов. Возможности и деструктивные функции вредоносных кодов.

Тема 2. Распространение вредоносного кода. 1 час.

Способы доставки вредоносных кодов. Исполняемые файлы и расширения вредоносных кодов. Вредоносная рассылка. Вредоносные скрипты. Способы выявления наличия вредоносных кодов на устройствах. Действия при обнаружении вредоносных кодов на устройствах.

Тема 3. Методы защиты от вредоносных программ. 2 час.

Способы защиты устройств от вредоносного кода. Антивирусные программы и их характеристики. Правила защиты от вредоносных кодов.

Тема 4. Распространение вредоносного кода для мобильных устройств. 1 час.

Расширение вредоносных кодов для мобильных устройств. Правила безопасности при установке приложений на мобильные устройства.

Выполнение и защита индивидуальных и групповых проектов. 3 часа.

Раздел 3 «Безопасность информации»

Тема 1. Социальная инженерия: распознать и избежать. 1 час.

Приемы социальной инженерии. Правила безопасности при виртуальных контактах.

Тема 2. Ложная информация в Интернете. 1 час.

Цифровое пространство как площадка самопрезентации, экспериментирования и освоения различных социальных ролей. Фейковые новости. Поддельные страницы.

Тема 3. Безопасность при использовании платежных карт в Интернете. 1 час.

Транзакции и связанные с ними риски. Правила совершения онлайн покупок. Безопасность банковских сервисов.

Тема 4. Беспроводная технология связи. 1 час.

Уязвимость Wi-Fi-соединений. Публичные и непубличные сети. Правила работы в публичных сетях.

Тема 5. Резервное копирование данных. 1 час.

Безопасность личной информации. Создание резервных копий на различных устройствах.

Тема 6. Основы государственной политики в области формирования культуры информационной безопасности. 2 час.

Доктрина национальной информационной безопасности. Обеспечение свободы и равенства доступа к информации и знаниям. Основные направления государственной политики в области формирования культуры информационной безопасности.

Выполнение и защита индивидуальных и групповых проектов. 3 часа.
Повторение, резерв. 3 часа.

7 класс (34 часа)

Раздел 1. «Безопасность общения»

Тема 1. Общение в социальных сетях и мессенджерах 8 часов

Социальная сеть. История социальных сетей. Мессенджеры. Назначение социальных сетей и мессенджеров. Пользовательский контент.

Тема 2. С кем безопасно общаться в интернете. 6 часов.

Персональные данные как основной капитал личного пространства в цифровом мире. Правила добавления друзей в социальных сетях. Профиль пользователя. Анонимные социальные сети.

Тема 3. Пароли для аккаунтов социальных сетей. 4 часа..

Сложные пароли. Онлайн генераторы паролей. Правила хранения паролей. Использование функции браузера по запоминанию паролей.

Тема 4. Безопасный вход в аккаунты. 6 часов.

Виды аутентификации. Настройки безопасности аккаунта. Работа на чужом компьютере с точки зрения безопасности личного аккаунта.

Тема 5. Настройки конфиденциальности в социальных сетях. 6 часов.

Настройки приватности и конфиденциальности в разных социальных сетях. Приватность и конфиденциальность в мессенджерах.

Тема 6. Публикация информации в социальных сетях. 6 часов.

Персональные данные. Публикация личной информации.

Тема 7. Кибербуллинг. 8 часов.

Определение кибербуллинга. Возможные причины кибербуллинга и как его избежать? Как не стать жертвой кибербуллинга. Как помочь жертве кибербуллинга.

Тема 8. Публичные аккаунты. 4 часа.

Настройки приватности публичных страниц. Правила ведения публичных страниц. Овершеринг.

Тема 9. Фишинг. 12 часов.

Фишинг как мошеннический прием. Популярные варианты распростра-нения фишинга. Отличие настоящих и фишинговых сайтов. Как защититься от фишеров в социальных сетях и мессенджерах.

Выполнение и защита индивидуальных и групповых проектов. 8 часов.

8 класс (34 часа

Раздел 2. «Безопасность устройств»

Тема 1. Повторение раздела 1. 6 часов.

Повторение раздела 1. «Безопасность общения»

Тема 2. Что такое вредоносный код. 4 часа.

Виды вредоносных кодов. Возможности и деструктивные функции вредоносных кодов.

Тема 3. Распространение вредоносного кода. 6 часов.

Способы доставки вредоносных кодов. Исполняемые файлы и расширения вредоносных кодов. Вредоносная рассылка. Вредоносные скрипты. Способы выявления наличия вредоносных кодов на устройствах. Действия при обнаружении вредоносных кодов на устройствах.

Тема 4. Методы защиты от вредоносных программ. 4 часа.

Способы защиты устройств от вредоносного кода. Антивирусные программы и их характеристики. Правила защиты от вредоносных кодов.

Тема 5. Распространение вредоносного кода для мобильных устройств. 4 часа.

Расширение вредоносных кодов для мобильных устройств. Правила безопасности при установке приложений на мобильные устройства.

Выполнение и защита индивидуальных и групповых проектов. 10 часов.

9 класс (34 часа)

Раздел 3 «Безопасность информации»

Тема 1. Повторение раздела 2. 4 часа.

Повторение раздела 2. «Безопасность устройств»

Тема 2. Социальная инженерия: распознать и избежать. 2 часа.

Приемы социальной инженерии. Правила безопасности при виртуальных контактах.

Тема 3. Ложная информация в Интернете. 2 часа.

Цифровое пространство как площадка самопрезентации, экспериментирования и освоения различных социальных ролей. Фейковые новости. Поддельные страницы.

Тема 4. Безопасность при использовании платежных карт в Интернете. 2 часа.

Транзакции и связанные с ними риски. Правила совершения онлайн по-купок. Безопасность банковских сервисов.

Тема 5. Беспроводная технология связи. 2 часа. Уязвимость Wi-Fi-соединений. Публичные и непубличные сети. Правила работы в публичных сетях.

Тема 6. Резервное копирование данных. 2 часа.

Безопасность личной информации. Создание резервных копий на различных устройствах.

Тема 7. Основы государственной политики в области формирования культуры информационной безопасности. 4 часа.

Доктрина национальной информационной безопасности. Обеспечение свободы и равенства доступа к информации и знаниям. Основные направления государственной политики в области формирования культуры информацион-ной безопасности.

Выполнение и защита индивидуальных и групповых проектов. 10 часов.

Повторение. Волонтерская практика. 6 часов.

Тематическое планирование учебного курса (Модуль 1)
5 класс

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

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

6 класс

№	Тема занятия	Кол-во часов
1	Вводное занятие. Техника безопасности в КК.	**1**
2	Как вести себя «в гостях» у сетевых друзей	**1**
3	Возможности и проблемы социальных сетей	**1**
4	Безопасный профиль в социальных сетях. Составление сети контактов	**1**
5	Защита персональных данных, почему она нужна. Категории персональных данных. Биометрические персональные данные	**1**
6	Информационная безопасность	**1**
7	Источники данных в Интернете: почта, сервисы обмена файлами и др. Хранение данных в Интернете	**1**
8	Комплекс упражнений при работе за компьютером	**1**
9	Воздействие на зрение ЭЛТ, жидкокристаллических, светодиодных, монохромных мониторов	**1**
10	Для чего может быть полезен ПК и Интернет (развивающие игры, обучение, общение и т.п.) и как польза превращается во вред	**1**
11	Киберкультура (массовая культура в сети) и личность	**1**
12	Психологическое воздействие информации на человека. Управление личностью через сеть	**1**
13	Психологическое воздействие информации на человека. Управление личностью через сеть	**1**
14	Методы защиты фото и видеоматериалов от копирования в сети	**1**
15	Защита от копирования контента сайта	**1**
16	Защита файлов. Права пользователей	**1**
17	Защита при загрузке и выключении компьютера	**1**
18	Безопасность при скачивании файлов	**1**
19	Безопасность при просмотре фильмов онлайн	**1**
20	Защита программ и данных от несанкционированного копирования. Организационные, юридические, программные и программно-аппаратные меры защиты	**1**
21	Защита программ и данных с помощью паролей, программных и электронных ключей, серийных номеров, переноса в онлайн и т.п. Неперемещаемые программы.	**1**
22	Как развивались вирусы	**1**

23	Могут ли вирусы воздействовать на аппаратуру ПК	**1**
24	Как вирусы воздействуют на файлы Проверка на наличие вирусов. Сканеры и др.	**1**
25	Может ли вирус воздействовать на рабочий стол	**1**
26	Источники заражения ПК	**1**
27	Антивирусное ПО, виды и назначение	**1**
28	Методы защиты от вирусов. Как распознаются вирусы	**1**
29	Виды мошенничества в Интернете. Фишинг (фарминг)	**1**
30	Виды мошенничества в Интернете. Фишинг (фарминг)	**1**
31	Азартные игры. Онлайн-казино. Букмекерские конторы. Предложения для «инвестирования» денег. Выигрыш в лотерею	**1**
32	Утечка и обнародование личных данных	**1**
33	Подбор и перехват паролей. Взломы аккаунтов в социальных сетях	**1**
34	Защита прав потребителей при использовании услуг Интернет Защита прав потребителей услуг провайдера	**1**

7 класс

№ п/п	Тема	Кол-во часов
	«Безопасность общения»	
1	Общение в социальных сетях и мессенджерах.	4
2	С кем безопасно общаться в интернете	2
3	Пароли для аккаунтов социальных сетей	2
4	Безопасный вход в аккаунты	2
5	Настройки конфиденциальности в социальных сетях	2
6	Публикация информации в социальных сетях	2
7	Кибербуллинг	4
8	Публичные аккаунты	2
9	Фишинг	6
10	Выполнение и защита индивидуальных и групповых проектов	8

8 класс

№ п/п	Тема	Кол-во часов
1	Повторение раздела 1. «Безопасность общения»	6
2	Что такое вредоносный код	4
3	Распространение вредоносного кода	6
4	Методы защиты от вредоносных программ	4
5	Распространение вредоносного кода для мобильных устройств	4
6	Выполнение и защита индивидуальных и групповых проектов	10

9 класс

№ п/п	Тема	Кол-во часов
1	Повторение раздела 2. «Безопасность устройств»	4
2	Социальная инженерия: распознать и избежать	2
3	Ложная информация в Интернете	2
4	Безопасность при использовании платежных карт в Интернете	2
5	Беспроводная технология связи	2
6	Резервное копирование данных	2
7	Основы государственной политики в области формирования культуры информационной безопасности	4
8	Выполнение и защита индивидуальных и групповых проектов	10
9	Повторение, волонтерская практика, резерв	6