МУНИЦИПАЛЬНОЕ АВТОНОМНОЕ ОБЩЕОБРАЗОВАТЕЛЬНОЕ УЧРЕЖДЕНИЕ
«ВОЛКОВСКАЯ СРЕДНЯЯ ОБЩЕОБРАЗОВАТЕЛЬНАЯ ШКОЛА»

Приложение № 1 к основной
образовательной программе основного
общего образования

ПРИНЯТО	СОГЛАСОВАНО	УТВЕРЖДЕНО
Педагогическим советом	Заместитель директора по УВР	Приказом директора
Протокол № 4	_____ Рявкина О.В.	МАОУ «Волковская СОШ»
от «30» мая 2022 г.	«27» мая 2022 г.	от «30» мая 2022 г. № 29-О
		_____ Ситникова М.М.

Программа
внеурочной деятельности
«Информационная безопасность»
7-9 классы

Количество часов 102
Уровень обучения - основное общее образование
Нормативный срок освоения - 3 года

Составитель:
Нурова Ситора Тавакаловна, учитель

с. Волковское

Структура рабочей программы

1. Планируемые результаты освоения учебного предмета
2. Содержание учебного предмета
3. Тематическое планирование с указанием количества часов, отводимых на освоение каждой темы.

1. ПЛАНИРУЕМЫЕ РЕЗУЛЬТАТЫ ОСВОЕНИЯ УЧЕБНОГО КУРСА 7-9 КЛАСС

Предметные результаты:

Научатся:

- анализировать доменные имена компьютеров и адреса документов в интернете;
- безопасно использовать средства коммуникации;
- безопасно вести и применять способы самозащиты при попытке мошенничества;
- безопасно использовать ресурсы интернета;

Получат возможность

Овладеть:

- приемами безопасной организации своего личного пространства данных с использованием индивидуальных накопителей данных, интернет-сервисов и т.п;
- основами самоконтроля, соблюдения норм информационной этики и права;
- навыками самостоятельного принятия решения и осуществления осознанного выбора в учебной и познавательной деятельности при формировании современной культуры безопасности в сети интернет;

Метапредметные результаты.

Межпредметные понятия.

В ходе изучения учебного курса обучающиеся усовершенствуют опыт проектной деятельности и навыки работы с информацией, в том числе в текстовом, табличном виде, виде диаграмм и пр.

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;
- формулировать учебные задачи как шаги достижения поставленной цели деятельности;
- обосновывать целевые ориентиры и приоритеты ссылками на ценности, указывая и обосновывая логическую последовательность шагов;
- определять необходимые действие(я) в соответствии с учебной и познавательной задачей и составлять алгоритм их выполнения;
- обосновывать и осуществлять выбор наиболее эффективных способов решения учебных и познавательных задач;
- определять/находить, в том числе из предложенных вариантов, условия для выполнения учебной и познавательной задачи;
- выстраивать жизненные планы на краткосрочное будущее (заявлять целевые ориентиры, ставить адекватные им задачи и предлагать действия, указывая и обосновывая логическую последовательность шагов);
- выбирать из предложенных вариантов и самостоятельно искать средства/ресурсы для решения задачи/достижения цели;
- составлять план решения проблемы (выполнения проекта, проведения исследования);
- определять потенциальные затруднения при решении учебной и познавательной задачи и находить средства для их устранения;

- описывать свой опыт, оформляя его для передачи другим людям в виде технологии решения практических задач определенного класса;
- определять совместно с педагогом и сверстниками критерии планируемых результатов и критерии оценки своей учебной деятельности;
- систематизировать (в том числе выбирать приоритетные) критерии планируемых результатов и оценки своей деятельности;
- отбирать инструменты для оценивания своей деятельности, осуществлять самоконтроль своей деятельности в рамках предложенных условий и требований;
- 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;
- устанавливать связь между полученными характеристиками продукта и характеристиками процесса деятельности и по завершении деятельности предлагать изменение характеристик процесса для получения улучшенных характеристик продукта;
- сверять свои действия с целью и, при необходимости, исправлять ошибки самостоятельно;
- определять критерии правильности (корректности) выполнения учебной задачи;
- анализировать и обосновывать применение соответствующего инструментария для выполнения учебной задачи;
- свободно пользоваться выработанными критериями оценки и самооценки, исходя из цели и имеющихся средств, различая результат и способы действий;
- оценивать продукт своей деятельности по заданным и/или самостоятельно определенным критериям в соответствии с целью деятельности;
- обосновывать достижимость цели выбранным способом на основе оценки своих внутренних ресурсов и доступных внешних ресурсов;
- фиксировать и анализировать динамику собственных образовательных результатов.
- наблюдать и анализировать собственную учебную и познавательную деятельность и деятельность других обучающихся в процессе взаимопроверки;
- соотносить реальные и планируемые результаты индивидуальной образовательной деятельности и делать выводы;
- принимать решение в учебной ситуации и нести за него ответственность.

Познавательные универсальные учебные действия

В результате освоения учебного курса обучающийся сможет:

- выделять общий признак двух или нескольких предметов или явлений, объяснять их сходство;
- объединять предметы и явления в группы по определенным признакам, сравнивать, классифицировать и обобщать факты и явления;
- 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;
- строить рассуждение на основе сравнения предметов и явлений, выделяя при этом общие признаки;
- излагать полученную информацию, интерпретируя ее в контексте решаемой задачи;
- самостоятельно указывать на информацию, нуждающуюся в проверке, предлагать и применять способ проверки достоверности информации;

- вербализовать эмоциональное впечатление, оказанное на него источником;
- объяснять явления, процессы, связи и отношения, выявляемые в ходе познавательной и исследовательской деятельности (приводить объяснение с изменением формы представления; объяснять, детализируя или обобщая; объяснять с заданной точки зрения);
- делать вывод на основе критического анализа разных точек зрения, подтверждать вывод собственной аргументацией или самостоятельно полученными данными;
- переводить сложную по составу (многоаспектную) информацию из графического или формализованного (символьного) представления в текстовое, и наоборот;
- анализировать/рефлексировать опыт разработки и реализации учебного проекта, исследования (теоретического, эмпирического) на основе предложенной проблемной ситуации, поставленной цели и/или заданных критериев оценки продукта/результата.
- критически оценивать содержание и форму текста;
- определять необходимые ключевые поисковые слова и запросы;
- осуществлять взаимодействие с электронными поисковыми системами, словарями;
- формировать множественную выборку из поисковых источников для объективизации результатов поиска;
- соотносить полученные результаты поиска со своей деятельностью.

Коммуникативные универсальные учебные действия

В результате освоения учебного курса обучающийся сможет:

- определять возможные роли в совместной деятельности;
- играть определенную роль в совместной деятельности;
- принимать позицию собеседника, понимая позицию другого, различать в его речи: мнение (точку зрения), доказательство (аргументы), факты; гипотезы, аксиомы, теории;
- определять свои действия и действия партнера, которые способствовали или препятствовали продуктивной коммуникации;
- строить позитивные отношения в процессе учебной и познавательной деятельности;
- корректно и аргументированно отстаивать свою точку зрения, в дискуссии уметь выдвигать контраргументы, перефразировать свою мысль (владение механизмом эквивалентных замен);
- критически относиться к собственному мнению, с достоинством признавать ошибочность своего мнения (если оно таково) и корректировать его;
- предлагать альтернативное решение в конфликтной ситуации;
- выделять общую точку зрения в дискуссии;
- договариваться о правилах и вопросах для обсуждения в соответствии с поставленной перед группой задачей;
- организовывать учебное взаимодействие в группе (определять общие цели, распределять роли, договариваться друг с другом и т. д.);
- устранять в рамках диалога разрывы в коммуникации, обусловленные непониманием/неприятием со стороны собеседника задачи, формы или содержания диалога;
- определять задачу коммуникации и в соответствии с ней отбирать речевые средства;
- отбирать и использовать речевые средства в процессе коммуникации с другими людьми (диалог в паре, в малой группе и т. д.);
- представлять в устной или письменной форме развернутый план собственной деятельности;
- соблюдать нормы публичной речи, регламент в монологе и дискуссии в соответствии с коммуникативной задачей;
- высказывать и обосновывать мнение (суждение) и запрашивать мнение партнера в рамках диалога;
- принимать решение в ходе диалога и согласовывать его с собеседником;

- создавать письменные «клишированные» и оригинальные тексты с использованием необходимых речевых средств;
- использовать вербальные средства (средства логической связи) для выделения смысловых блоков своего выступления;
- использовать невербальные средства или наглядные материалы, подготовленные/отобранные под руководством учителя;
- 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, созданиепрезентаций 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 ценности безопасного образа жизни; интериоризация правил индивидуального и коллективного безопасного поведения в информационно-телекоммуникационной среде.

2. СОДЕРЖАНИЕ УЧЕБНОГО КУРСА

7 класс

Модуль 1. Общие сведения о безопасности ПК и Интернета (5 часов).

Как работают мобильные устройства. Угрозы для мобильных устройств.

Распространение вредоносных файлов через приложения для смартфонов и планшетов (скачивание фотографий, музыки, игр).

Виды защиты киберпространства (что такое несанкционированный доступ, разрушение и утрата информации, искажение информации).

Кто обеспечивает защиту киберпространства.

Что такое геоинформационные системы (ГИС). Глобальные информационные Сети по стихийным бедствиям.

Модуль 2. Техника безопасности и экология (5 часов).

Компьютер и мобильные устройства в чрезвычайных ситуациях. Дополнения к ДТП. Компьютер и мобильные (сотовые) устройства в правилах безопасности.

Компьютеры и мобильные устройства в экстремальных условиях.

Везде ли есть Интернет. ТБ при работе с мобильными устройствами.

Первая помощь при проблемах в интернете (службы помощи).

Воздействие радиоволн на здоровье и окружающую среду (Wi-Fi, Bluetooth, GSM).

Модуль 3. Проблемы Интернет-зависимости (2 часа).

Виды Интернет-зависимости.

Компьютер и зрение.

Модуль 4. Методы обеспечения безопасности ПК и Интернета.

Вирусы и антивирусы (8 часов).

Вирусы и антивирусы.

Как распространяются вирусы.

Источники и причины заражения.

Скорая компьютерная помощь. Признаки заражения компьютера.

Что такое антивирусная защита. Как лечить компьютер.

Защита мобильных устройств.

Как защитить данные от потерь. Копирование и восстановление. Всегда ли можно спасти свои данные.

Защита файлов. Что такое право доступа.

Защита детей в социальных сетях. ПО для родителей. Ограничение времени нахождения в сети.

Модуль 5. Мошеннические действия в Интернете. Киберпреступления (2 часа).

Опасности мобильной связи. Предложения по установке вредоносных приложений. Мошеннические СМС.

Прослушивание разговоров. Определение местоположения телефона.

Модуль 6. Сетевой этикет. Психология и сеть (10 часов).

Что такое личные данные. Все, что выложено в Интернет, может стать известно всем.

«Лишняя информация» о себе и других в Интернете. Какая информация принадлежит вам.

Анонимность в сети.

Что такое этикет. Виды этикета (личный, деловой, письменный, дискуссионный и пр.). Различия этикета в разных странах.

Как появился нетикет, что это такое. Общие правила сетевого этикета.

Личное общение и общение в группе – чем они отличаются (чаты, форумы, службы мгновенных сообщений).

Этика дискуссий. Взаимное уважение при интернет-общении.

Этикет и безопасность. Эмоции в сети, их выражение.

Реальная и виртуальная личность, реальные встречи с виртуальными знакомыми и их опасность, угрозы и оскорбления – чем это может закончиться.

Если вы стали жертвой компьютерной агрессии: службы помощи.

Модуль 7. Правовые аспекты защиты киберпространства (2 часа).

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

Обобщение материала курса. Игра-квест «Знатоки кибербезопасности».

8 класс

Модуль 1. Общие сведения о безопасности ПК и Интернета (5 часов).

Информационная безопасность

Защита персональных данных, почему она нужна. Категории персональных данных. Биометрические персональные данные.

Источники данных в Интернете: почта, сервисы обмена файлами и др. Хранение данных в Интернете.

Возможности и проблемы социальных сетей.

Безопасный профиль в социальных сетях. Составление сети контактов.

Модуль 2. Техника безопасности и экология (2 часа).

Комплекс упражнений при работе за компьютером.

Воздействие на зрение ЭЛТ, жидкокристаллических, светодиодных, монохромных мониторов.

Модуль 3. Проблемы Интернет-зависимости (3 часа).

Для чего может быть полезен ПК и Интернет (развивающие игры, обучение, общение и т.п.) и как польза превращается во вред.

Киберкультура (массовая культура в сети) и личность.

Психологическое воздействие информации на человека. Управление личностью через сеть.

Модуль 4. Методы обеспечения безопасности ПК и Интернета.

Вирусы и антивирусы (16 часов).

Защита файлов. Права пользователей.

Защита при загрузке и выключении компьютера.

Безопасность при скачивании файлов.

Безопасность при просмотре фильмов онлайн.

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. Неперемещаемые программы.

Методы защиты фото и видеоматериалов от копирования в сети.

Защита от копирования контента сайта.

Как развивались вирусы.

Могут ли вирусы воздействовать на аппаратуру ПК.

Как вирусы воздействуют на файлы.

Проверка на наличие вирусов. Сканеры и др.

Может ли вирус воздействовать на рабочий стол.

Источники заражения ПК.

Антивирусное ПО, виды и назначение.

Методы защиты от вирусов. Как распознаются вирусы.

Модуль 5. Мошеннические действия в Интернете. Киберпреступления (4 часа).

Утечка и обнародование личных данных.

Подбор и перехват паролей. Взломы аккаунтов в социальных сетях.

Виды мошенничества в Интернете. Фишинг (фарминг).

Азартные игры. Онлайн-казино. Букмекерские конторы. Предложения для «инвестирования» денег. Выигрыш в лотерею.

Модуль 6. Сетевой этикет. Психология и сеть (1 час).

Психологическая обстановка в Интернете: грифинг, кибербуллинг, кибер-моббинг, троллинг, буллицид.

Модуль 7. Правовые аспекты защиты киберпространства (3 часа).

Защита прав потребителей при использовании услуг Интернет.

Защита прав потребителей услуг провайдера.

Обобщение материала курса. Игра-квест «Знатоки кибербезопасности».

9 класс

Модуль 1. Общие сведения о безопасности ПК и Интернета (11 часов).

Защита киберпространства как комплекс мероприятий, направленных на обеспечение информационной безопасности. Аспекты кибербезопасности.

Компьютерная и информационная безопасность, обнаружение проблем сети, восстановление параметров систем, средства защиты от несанкционированного доступа к данным, криптографическая защита информации.

Что такое защищенная информационная среда. Защита каналов передачи данных, средства предотвращения утечки информации, защита информации от НСД (антивирусная защита, средства контроля защищенности, средства обнаружения и предупреждения атак), средства аутентификации.

Организационно-технические меры защиты информационной среды. Системы охранной сигнализации, видеонаблюдение, контроль и управление доступом, средства уничтожения

информации, средства резервного копирования и восстановления.

Требования к безопасности информации: сохранение целостности, конфиденциальности и доступности. Определения по ГОСТ РВ 51987-2002 «Информационная технология. Комплекс стандартов на автоматизированные системы. Типовые требования и показатели качества функционирования информационных систем. Общие положения».

Признаки нарушения целостности программ и данных. Способы нарушения целостности информации. Признаки и способы нарушения конфиденциальности. Признаки и способы нарушения доступности информации.

Безопасность мобильных устройств в информационных системах. Источники заражения мобильных устройств (веб-ресурсы, магазины приложений, ботнеты).

Угрозы безопасности в сетях WiFi. Методы защиты сетей WiFi.

Угрозы информации (техногенные, случайные и преднамеренные; природные). Неосторожность пользователя как одна из угроз для информационной безопасности.

Меры кибербезопасности для конечных пользователей. Использование рекомендованных версий операционных систем и приложений, использование антивирусных средств, настройка веб-браузеров, блокировка скриптов, использование фильтров фишинга, межсетевых экранов. Автоматическое обновление ПО.

Киберугрозы Интернета (кибервойны, манипулирование людьми, зависимость, вирусные атаки, отсутствие приватности).

Модуль 2. Техника безопасности и экология (3 часа).

Кибератаки на инфраструктуру.

Компьютер в режиме труда и отдыха. Информационная перегрузка.

Влияние компьютера на репродуктивную систему.

Модуль 3. Проблемы Интернет-зависимости (2 часа).

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).

Модуль 4. Методы обеспечения безопасности ПК и Интернета.

Вирусы и антивирусы (7 часов).

Проблемы безопасности инфраструктуры Интернета (протоколы маршрутизации сети, система доменных имен, средства маршрутизации и т.п.). Методы защиты.

Проверка подлинности (аутентификация) в Интернете.

Меры безопасности для пользователя WiFi. Настройка безопасности.

Вирусы для мобильных устройств (мобильные банкеры и др.).

Настройка компьютера для безопасной работы.

Ошибки пользователя (установка нескольких антивирусов, установка слишком большого числа программ, отсутствие резервного копирования и т.п.).

Меры личной безопасности при сетевом общении. Настройки приватности в социальных сетях.

Модуль 5. Мошеннические действия в Интернете. Киберпреступления (7 часов).

Мошеннические действия в сети. Предложения о разблокировании программ (блокировщики windows). Ложные антивирусы.

Подмена страниц в интернете (сайты-клоны). Фальшивые файлообменники.

Мошеннические действия в сети. Сбор «пожертвований» на благотворительность. «Легкий заработок» в Интернете. Пирамиды.

Что такое электронный кошелек – удобства и проблемы безопасности. «Обменники» для электронных денег.

Мошенничество при распространении «бесплатного» ПО. Продажа «обучающих курсов» для бизнеса.

Платные предложения работы. Платный просмотр видеоматериалов.

Технологии манипулирования в Интернете.

Модуль 6. Сетевой этикет. Психология и сеть (1 час).

Безопасная работа в сети в процессе сетевой коммуникации (чаты, форумы, конференции, скайп, социальные сети и пр.). Сетевой этикет. Термины сетевого этикета: оверквотинг, флейм, флуд, оффтопик, смайлики и др.

Модуль 7. Правовые аспекты защиты киберпространства (3 часа).

Как расследуются преступления в сети.

Ответственность за интернет-мошенничество.

Обобщение материала курса. Игра-квест «Знатоки кибербезопасности».

3. ТЕМАТИЧЕСКОЕ ПЛАНИРОВАНИЕ

7 класс

№ урока	Тема	Кол-во часов
	Общие сведения о безопасности ПК и Интернета	**5**
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 (ГИС). Глобальные информационные Сети по стихийным бедствиям.	
	Техника безопасности и экология.	**5**
6	Компьютер и мобильные устройства в чрезвычайных ситуациях. Дополнения к ДТП. Компьютер и мобильные (сотовые) устройства в правилах безопасности.	
7	Компьютеры и мобильные устройства в экстремальных условиях.	
8	Везде ли есть Интернет. ТБ при работе с мобильными устройствами.	
9	Первая помощь при проблемах в интернете (службы помощи).	
10	Воздействие радиоволн на здоровье и окружающую среду (Wi-Fi, Bluetooth, GSM).	
	Проблемы Интернет-зависимости.	**2**
11	Виды Интернет-зависимости.	
12	Компьютер и зрение.	
	Методы обеспечения безопасности ПК и Интернета. Вирусы и антивирусы.	**8**
13	Как распространяются вирусы.	
14	Источники и причины заражения.	
15	Скорая компьютерная помощь. Признаки заражения компьютера.	
16	Что такое антивирусная защита. Как лечить компьютер.	
17	Защита мобильных устройств.	
18	Как защитить данные от потерь. Копирование и восстановление. Всегда ли можно спасти свои данные.	
19	Защита файлов. Что такое право доступа.	
20	Защита детей в социальных сетях. ПО для родителей. Ограничение времени нахождения в сети.	
	Мошеннические действия в Интернете. Киберпреступления.	**2**
21	Опасности мобильной связи. Предложения по установке вредоносных приложений. Мошеннические СМС.	
22	Прослушивание разговоров. Определение местоположения телефона.	

	Сетевой этикет. Психология и сеть.	**10**
23	Что такое личные данные. Все, что выложено в Интернет, может стать известно всем.	
24	«Лишняя информация» о себе и других в Интернете. Какая информация принадлежит вам.	
25	Анонимность в сети.	
26	Что такое этикет. Виды этикета (личный, деловой, письменный, дискуссионный и пр.). Различия этикета в разных странах.	
27	Как появился нетикет, что это такое. Общие правила сетевого этикета.	
28	Личное общение и общение в группе – чем они отличаются (чаты, форумы, службы мгновенных сообщений).	
29	Этика дискуссий. Взаимное уважение при интернет-общении.	
30	Этикет и безопасность. Эмоции в сети, их выражение.	
31	Реальная и виртуальная личность, реальные встречи с виртуальными знакомыми и их опасность, угрозы и оскорбления – чем это может закончиться.	
32	Если вы стали жертвой компьютерной агрессии: службы помощи.	
	Правовые аспекты защиты киберпространства.	**2**
33	Собственность в Интернете. Авторское право. Интеллектуальная собственность. Платная и бесплатная информация.	
34	Обобщение материала курса. Игра-квест «Знатоки кибербезопасности».	

8 класс

№ урока	Тема	Кол-во часов
	Общие сведения о безопасности ПК и Интернета	**5**
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. Хранение данных в Интернете.	
4	Возможности и проблемы социальных сетей.	
5	Безопасный профиль в социальных сетях. Составление сети контактов.	
	Техника безопасности и экология.	**2**
6	Комплекс упражнений при работе за компьютером.	
7	Воздействие на зрение ЭЛТ, жидкокристаллических, светодиодных, монохромных мониторов.	
	Проблемы Интернет-зависимости.	**3**
8	Для чего может быть полезен ПК и Интернет (развивающие игры, обучение, общение и т.п.) и как польза превращается во вред.	
9	Киберкультура (массовая культура в сети) и личность.	
10	Психологическое воздействие информации на человека. Управление личностью через сеть.	
	Методы обеспечения безопасности ПК и Интернета. Вирусы и антивирусы.	**16**
11	Защита файлов. Права пользователей.	
12	Защита при загрузке и выключении компьютера.	
13	Безопасность при скачивании файлов.	
14	Безопасность при просмотре фильмов онлайн.	
15	Защита программ и данных от несанкционированного копирования. Организационные, юридические, программные и программно-аппаратные	

	меры защиты.	
16	Защита программ и данных с помощью паролей, программных и электронных ключей, серийных номеров, переноса в онлайн и т.п. Неперемещаемые программы.	
17	Методы защиты фото и видеоматериалов от копирования в сети.	
18	Защита от копирования контента сайта.	
19	Как развивались вирусы.	
20	Могут ли вирусы воздействовать на аппаратуру ПК.	
21	Как вирусы воздействуют на файлы.	
22	Проверка на наличие вирусов. Сканеры и др.	
23	Может ли вирус воздействовать на рабочий стол.	
24	Источники заражения ПК.	
25	Антивирусное ПО, виды и назначение.	
26	Методы защиты от вирусов. Как распознаются вирусы.	
	Мошеннические действия в Интернете. Киберпреступления.	**4**
27	Утечка и обнародование личных данных.	
28	Подбор и перехват паролей. Взломы аккаунтов в социальных сетях.	
29	Виды мошенничества в Интернете. Фишинг (фарминг).	
30	Азартные игры. Онлайн-казино. Букмекерские конторы. Предложения для «инвестирования» денег. Выигрыш в лотерею.	
	Сетевой этикет. Психология и сеть.	**1**
31	Психологическая обстановка в Интернете: грифинг, кибербуллинг, кибер-моббинг, троллинг, буллицид.	
	Правовые аспекты защиты киберпространства.	**3**
32	Защита прав потребителей при использовании услуг Интернет.	
33	Защита прав потребителей услуг провайдера.	
34	Обобщение материала курса. Игра-квест «Знатоки кибербезопасности».	

9 класс

№ урока	Тема	Кол-во часов
	Общие сведения о безопасности ПК и Интернета.	**11**
1	Защита киберпространства как комплекс мероприятий, направленных на обеспечение информационной безопасности. Аспекты кибербезопасности.	
2	Компьютерная и информационная безопасность, обнаружение проблем сети, восстановление параметров систем, средства защиты от несанкционированного доступа к данным, криптографическая защита информации.	
3	Что такое защищенная информационная среда. Защита каналов передачи данных, средства предотвращения утечки информации, защита информации от НСД (антивирусная защита, средства контроля защищенности, средства обнаружения и предупреждения атак), средства аутентификации.	
4	Организационно-технические меры защиты информационной среды. Системы охранной сигнализации, видеонаблюдение, контроль и управление доступом, средства уничтожения информации, средства резервного копирования и восстановления.	
5	Требования к безопасности информации: сохранение целостности, конфиденциальности и доступности. Определения по ГОСТ РВ 51987-2002 «Информационная технология. Комплекс стандартов на автоматизированные системы. Типовые требования и показатели качества	

	функционирования информационных систем. Общие положения».	
6	Признаки нарушения целостности программ и данных. Способы нарушения целостности информации. Признаки и способы нарушения конфиденциальности. Признаки и способы нарушения доступности информации.	
7	Безопасность мобильных устройств в информационных системах. Источники заражения мобильных устройств (веб-ресурсы, магазины приложений, ботнеты).	
8	Угрозы безопасности в сетях WiFi. Методы защиты сетей WiFi.	
9	Угрозы информации (техногенные, случайные и преднамеренные; природные). Неосторожность пользователя как одна из угроз для информационной безопасности.	
10	Меры кибербезопасности для конечных пользователей. Использование рекомендованных версий операционных систем и приложений, использование антивирусных средств, настройка веб-браузеров, блокировка скриптов, использование фильтров фишинга, межсетевых экранов. Автоматическое обновление ПО.	
11	Киберугрозы Интернета (кибервойны, манипулирование людьми, зависимость, вирусные атаки, отсутствие приватности).	
	Техника безопасности и экология.	**3**
12	Кибератаки на инфраструктуру.	
13	Компьютер в режиме труда и отдыха. Информационная перегрузка.	
14	Влияние компьютера на репродуктивную систему.	
	Проблемы Интернет-зависимости.	**2**
15	Интернет- и компьютерная зависимость (аддикция). Критерии зависимости с точки зрения психологов (приоритетность, изменения настроения, толерантность, симптом разрыва, конфликт, рецидив). Как развивается зависимость.	
16	Типы интернет-зависимости (пристрастие к работе с компьютером, к навигации и поиску информации, игромания и электронные покупки, зависимость от сетевого общения, сексуальные зависимости).	
	Методы обеспечения безопасности ПК и Интернета. Вирусы и антивирусы.	**7**
17	Проблемы безопасности инфраструктуры Интернета (протоколы маршрутизации сети, система доменных имен, средства маршрутизации и т.п.). Методы защиты.	
18	Проверка подлинности (аутентификация) в Интернете.	
19	Меры безопасности для пользователя WiFi. Настройка безопасности.	
20	Вирусы для мобильных устройств (мобильные банкеры и др.).	
21	Настройка компьютера для безопасной работы.	
22	Ошибки пользователя (установка нескольких антивирусов, установка слишком большого числа программ, отсутствие резервного копирования и т.п.).	
23	Меры личной безопасности при сетевом общении. Настройки приватности в социальных сетях.	
	Мошеннические действия в Интернете. Киберпреступления.	**7**
24	Мошеннические действия в сети. Предложения о разблокировании программ (блокировщики windows). Ложные антивирусы.	
25	Подмена страниц в интернете (сайты-клоны). Фальшивые файлообменники.	
26	Мошеннические действия в сети. Сбор «пожертвований» на благотворительность. «Легкий заработок» в Интернете. Пирамиды.	

27	Что такое электронный кошелек – удобства и проблемы безопасности. «Обменники» для электронных денег.	
28	Мошенничество при распространении «бесплатного» ПО. Продажа «обучающих курсов» для бизнеса.	
29	Платные предложения работы. Платный просмотр видеоматериалов.	
30	Технологии манипулирования в Интернете.	
	Сетевой этикет. Психология и сеть.	**1**
31	Безопасная работа в сети в процессе сетевой коммуникации (чаты, форумы, конференции, скайп, социальные сети и пр.). Сетевой этикет. Термины сетевого этикета: оверквотинг, флейм, флуд, оффтопик, смайлики и др.	
	Правовые аспекты защиты киберпространства.	**3**
32	Как расследуются преступления в сети.	
33	Ответственность за интернет-мошенничество.	
34	Обобщение материала курса. Игра-квест «Знатоки кибербезопасности».	