МИНИСТЕРСТВО ПРОСВЕЩЕНИЯ РОССИЙСКОЙ ФЕДЕРАЦИИ
Министерство образования и науки Самарской области
Кинельское управление министерства образования и науки Самарской области
ГБОУ СОШ с. Георгиевка

РАССМОТРЕНО	СОГЛАСОВАНО	УТВЕРЖДЕНО
на заседании МО "Точных наук" Руководитель МО Цыганова Э.В. Пр.№1 от 28.08.23г.	заместителем директора по УВР Калентьева Ю.В. от 28.08.23г.	Директор ГБОУ СОШ с.Георгиевка Ивлиева Р.К. № 71 ОД от 29.08.23г.

ЭП

C=RU, O=ГБОУ СОШ с. Георгиевка, CN=Ивлиева Р.К., E=georg_sch_knl@samara.edu.ru 0090b6f41e18d0dc73 2023.08.29 13:36:45+04'00'

Рабочая программа
курса внеурочной деятельности

Информационная безопасность

основного общего образования
обще-интеллектуального направления

7 – 9 класс

Нормативную правовую основу настоящей примерной образовательной программы по учебному курсу «Информационная безопасность» составляют следующие документы:

— Федеральный закон от 29 декабря 2012 г. № 273-ФЗ «Об образовании в Российской Федерации»;

— ФГОС основного общего образования;

— ООП основного общего образования;

— распоряжение Правительства РФ от 2 декабря 2015 г. № 2471-р «Об утверждении Концепции информационной безопасности детей»;

— Указ Президента РФ от 5 декабря 2016 г. № 646 «Об утверждении Доктрины информационной безопасности Российской Федерации»;

— Указ Президента РФ от 9 мая 2017 г. № 203 «О Стратегии развития информационного общества в Российской Федерации на 2017—2030 годы»;

— Перечень поручений по реализации Послания Президента Федеральному Собранию от 27 февраля 2019 г. Пр-294.

Программа внеурочной деятельности по учебному курсу «Информационная безопасность» (далее — программа) разработана на основе требований федерального государственного образовательного стандарта основного общего образования к результатам их освоения в части предметных результатов в рамках формирования ИКТ-компетентностей обучающихся по работе с информацией в глобальном информационном пространстве, а также личностных и метапредметных результатов в рамках социализации обучающихся в информационном мире и формирования культуры информационной безопасности обучающихся.

Программа включает пояснительную записку, в которой раскрываются цели изучения, общая характеристика и определяется место учебного курса «Информационная безопасность» в учебном плане, раскрываются основные подходы к отбору содержания и характеризуются его основные содержательные линии.

Программа устанавливает планируемые результаты освоения программы по курсу информационной безопасности для основного общего образования для 7—9 классов.

Программа определяет примерное календарное планирование учебного курса для указанных возрастных групп общего образования с указанием примерных часов на каждую тему по модулям программы в рамках их интеграции в дополнение к программам отдельных учебных предметов, а также в рамках программы воспитания (социализации) обучающихся или как отдельного учебного курса из часов, формируемых образовательной организацией.

ПОЯСНИТЕЛЬНАЯ ЗАПИСКА

Программа учебного курса «Информационная безопасность» разработана для организаций, реализующих программы общего образования. *В ней учтены приоритеты научно-технологического развития Российской Федерации* (Пр-294, п. 2а-16) и обновление программы воспитания и социализации обучающихся в школах Российской Федерации.

Цели изучения учебного курса «Информационная безопасность»

Безопасность в сети Интернет в свете быстрого развития информационных технологий, их глобализации, использования облачных технологий и повсеместного массового распространения среди детей мобильных персональных цифровых устройств доступа к сети Интернет, появления большого количества сетевых сервисов и интернет-коммуникаций, в том числе закрытых сетевых сообществ неизвестного толка, а также общедоступных и зачастую навязчивых интернет-ресурсов (СМИ, реклама, спам), содержащих негативный и агрессивный контент, расширения угроз новых сетевых средств вмешательства в личное информационное пространство на персональных устройствах, работающих в Интернете, а также в связи с массовым использованием детьми электронных социальных/банковских карт, имеющих персональные настройки доступа к ним, резко повышает потребность в воспитании у обучающихся культуры информационной безопасности в целях предотвращения негативных последствий массового использования Интернета детьми и их защиты от агрессивной и противоправной информации.

Программа учебного курса информационной безопасности имеет высокую актуальность и отражает важные вопросы безопасной работы с новыми формами коммуникаций и услуг цифрового мира: потребность в защите персональной информации, угрозы, распространяемые глобальными средствами коммуникаций Интернета и мобильной связи, использующими рассылки сообщений, электронную почту, информационно-коммуникативные ресурсы взаимодействия в сети Интернет через массово доступные услуги электронной коммерции, социальные сервисы, сетевые объединения и сообщества, ресурсы для досуга (компьютерные игры, видео и цифровое телевидение, цифровые средства массовой информации и новостные сервисы), а также повсеместное встраивание дистанционных ресурсов и технологий в учебную деятельность, использующую поиск познавательной и учебной информации, общение в социальных сетях, получение и передачу файлов, размещение личной информации в коллективных сервисах. Помимо профилактики информационных угроз и противоправных действий через ресурсы в сети Интернет и мобильные сети, крайне актуально использовать коммуникации для привлечения обучающихся к информационно-учебной и познавательно-творческой активности по использованию позитивных интернет-ресурсов: учебных, культурных, научно-популярных, интеллектуальных, читательских, медийных, правовых, познавательных и специализированных социальных сообществ и сервисов для детских объединений и творческих мероприятий для детей и молодежи.

При реализации требований безопасности в сети Интернет для любого пользователя, будь то школьник или учитель, образовательное учреждение должно обеспечивать защиту конфиденциальных сведений, представляющих собой в том числе персональные данные школьника, и предотвращать доступ к противоправной негативной информации. Но включение детей в интернет-взаимодействие наиболее активно осуществляется вне школы без надлежащего надзора со стороны взрослых.

В связи с этим в настоящее время необходимо особое внимание уделять воспитанию у детей *культуры информационной безопасности* при работе в сети Интернет вне школы с участием родителей. Для этого следует проводить непрерывную образовательно-просветительскую работу с детьми, формировать у обучающихся ответственное и критическое отношение к источникам информации, правовую культуру в сфере защиты от негативной информации и противоправных действий средствами коммуникаций, в том числе внимательно относиться к использованию детьми личных устройств мобильной связи, домашнего компьютера с Интернетом, телевизора, подключенного к Интернету, использовать дома программные средства защиты от доступа детей к негативной информации или информации по возрастным признакам (возраст+). Научить школьника правильно ориентироваться в большом количестве ресурсов в сети Интернет — важная задача для вовлечения детей в современную

цифровую образовательную среду, отвлечения их от бесполезного контента и игромании, бесцельной траты времени в социальных сетях и сервисах мобильной связи.

Главная цель курса — обеспечить социальные аспекты информационной безопасности в воспитании культуры информационной безопасности у школьников в условиях цифрового мира, включение на регулярной основе цифровой гигиены в контекст воспитания и обучения детей, формирование у выпускника школы правовой грамотности по вопросам информационной безопасности, которые влияют на социализацию детей в информационном обществе, формирование личностных и метапредметных результатов воспитания и обучения детей:

— формировать понимание сущности и воспитывать необходимость принятия обучающимися таких ценностей, как ценность человеческой жизни, свободы, равноправия и достоинства людей, здоровья, опыта гуманных, уважительных отношений с окружающими;

— создавать педагогические условия для формирования правовой и информационной культуры обучающихся, развития у них критического отношения к информации, ответственности за поведение в сети Интернет и последствия деструктивных действий, формирования мотивации к познавательной, а не игровой деятельности, воспитания отказа от пустого времяпрепровождения в социальных сетях, осознания ценности живого человеческого общения;

— формировать отрицательное отношение ко всем проявлениям жестокости, насилия, нарушения прав личности, экстремизма во всех его формах в сети Интернет;

— мотивировать обучающихся к осознанному поведению на основе понимания и принятия ими морально-правовых регуляторов жизни общества и государства в условиях цифрового мира;

— научить молодых людей осознавать важность проектирования своей жизни и будущего своей страны — России в условиях развития цифрового мира, ценность ИКТ для достижения высоких требований к обучению профессиям будущего в мире, принимать средства в Интернете как среду созидания, а не разрушения человека и общества.

Место учебного курса «Информационная безопасность» в учебном плане

Особенностью программы курса является ее поэтапное развитие для разных возрастных групп обучающихся основного общего образования с учетом из возрастных особенностей. Программа курса ориентирована на включение в контекст обучения и воспитания новых видов информационных угроз и средств противодействия им.

Данный курс реализуется в рамках социального направления внеурочной деятельности и рассчитан на 1 час в неделю с 7 по 9 класс (34 часа за год в каждом классе, всего 102 часа).

Программа учебного курса поддерживается электронными ресурсами на основе документальных фильмов, анимационных ресурсов и электронных практикумов в открытом доступе от ИТ-компаний Российской Федерации в рамках их участия в проектах по информационной безопасности для детей. В основе курса лежат технические, этические и правовые нормы соблюдения информационной безопасности, установленные контролирующими и правоохранительными органами, а также практические рекомендации ведущих ИТ-компаний и операторов мобильной связи Российской Федерации.

Общая характеристика учебного курса «Информационная безопасность»

Начинать обучение по курсу информационной безопасности крайне актуально по острым проблемным ситуациям в условиях присутствия в жизни детей персональных устройств работы в сети Интернет и мобильных сетях связи, а также для содействия при

использовании детьми Интернета для обучения, творческого и развивающего досуга, познавательной деятельности. Программа направлена на решение вопросов массового формирования культуры информационной безопасности школьников, которые живут в современном информационном обществе, стремительно расширяющем общедоступные коммуникации в Интернете.

Проникновение мобильных устройств с доступом к Интернету в быт и досуг детей обострило проблему интернет-зависимости, игромании, зависимости от социальных сетей, необоснованного доверия посторонним людям в сети и, как следствие, незащищенности детей от атак мошенников, преступников, агрессивно настроенных людей, включая вовлечение детей в теневые, закрытые субкультуры, несущие угрозу здоровью и даже жизни ребенка.

Курс «Информационная безопасность» структурирован по модульному принципу. Он включает в себя 7 модулей:

- Общие сведения о безопасности ПК и Интернета
- Техника безопасности и экология
- Проблемы Интернет-зависимости
- Методы обеспечения безопасности ПК и Интернета. Вирусы и антивирусы
- Мошеннические действия в Интернете. Киберпреступления
- Сетевой этикет. Психология и сеть
- Правовые аспекты защиты киберпространства

СОДЕРЖАНИЕ

УЧЕБНОГО КУРСА «ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ»

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».

ПЛАНИРУЕМЫЕ РЕЗУЛЬТАТЫ ОБУЧЕНИЯ ПО ПРОГРАММЕ

Программа учебного курса «Информационная безопасность» отражает в содержании цели поддержки и сопровождения безопасной работы с информацией в учебно-познавательной, творческой и досуговой деятельности (планируемые личностные, метапредметные и предметные результаты освоения курса).

В соответствии с федеральным государственным образовательным стандартом основного общего образования необходимо сформировать у обучающихся с учетом возрастных особенностей на каждом уровне общего образования такие *личностные результаты*, которые позволят им грамотно ориентироваться в информационном мире с учетом имеющихся в нем угроз:

— принимать ценности человеческой жизни, семьи, гражданского общества, многонационального российского народа, человечества;

— быть социально активными, уважающими закон и правопорядок, соизмеряющими свои поступки с нравственными ценностями, осознающими свои обязанности перед семьей, обществом, Отечеством;

— уважать других людей, уметь вести конструктивный диалог, достигать взаимопонимания, сотрудничать для достижения общих результатов;

— осознанно выполнять правила здорового образа жизни, безопасного для человека и окружающей его среды.

В рамках достижения этих личностных результатов при реализации программы курса информационной безопасности наиболее актуально в условиях быстро меняющегося и несущего в себе угрозы информационного мира обеспечить:

— развитие морального сознания и компетентности в решении моральных проблем на основе личностного выбора, формирование нравственных чувств и нравственного поведения, осознанного и ответственного отношения к собственным поступкам;

— формирование ценности здорового и безопасного образа жизни; усвоение правил индивидуального и коллективного безопасного поведения в чрезвычайных ситуациях, угрожающих жизни и здоровью людей.

В результате освоения программы курса информационной безопасности акцентируется внимание на *метапредметных результатах* освоения основной образовательной программы:

— освоение социальных норм, правил поведения, ролей и форм социальной жизни в группах и сообществах, включая взрослые и социальные сообщества; участие в школьном самоуправлении и общественной жизни в пределах возрастных компетенций с учетом региональных, этнокультурных, социальных и экономических особенностей;

— формирование коммуникативной компетентности в общении и сотрудничестве со сверстниками, детьми старшего и младшего возраста, взрослыми в процессе образовательной, общественно полезной, учебно-исследовательской, творческой и других видов деятельности;

— умение использовать средства информационно-коммуникационных технологий (ИКТ) в решении когнитивных, коммуникативных и организационных задач с соблюдением требований эргономики, техники безопасности, гигиены, ресурсосбережения, правовых и этических норм, норм информационной безопасности.

Планируется достижение *предметных результатов*, актуальных для курса информационной безопасности в интеграции с предметами «Информатика» и (или) «ОБЖ» для 7—9 классов.

— понимание личной и общественной значимости современной культуры безопасности жизнедеятельности;

— знание основных опасных и чрезвычайных ситуаций социального характера, включая экстремизм и терроризм, и их последствий для личности, общества и государства; формирование антиэкстремистской и антитеррористической личностной позиции;

— знание и умение применять меры безопасности и правила поведения в условиях опасных и чрезвычайных ситуаций.

— формирование навыков и умений безопасного и целесообразного поведения при работе с компьютерными программами и в Интернете, умения соблюдать нормы информационной этики;

— умение принимать обоснованные решения в конкретной опасной ситуации с учетом реально складывающейся обстановки и индивидуальных возможностей.

В результате освоения программы курса с учетом возрастных групп выпускник освоит жизненно важные практические компетенции.

Выпускник научится понимать:

— источники информационных угроз, вредоносные программы и нежелательные рассылки, поступающие на мобильный телефон, планшет, компьютер;

— роль близких людей, семьи, правоохранительных органов для устранения проблем и угроз в сети Интернет и мобильной телефонной связи, телефоны экстренных служб;

— виды информационных угроз, правила поведения для защиты от угроз, виды правовой ответственности за проступки и преступления в сфере информационной безопасности;

— проблемные ситуации и опасности в сетевом взаимодействии и правила поведения в проблемных ситуациях, ситуациях профилактики и предотвращения опасности;

— этикет сетевого взаимодействия, правовые нормы в сфере информационной

безопасности;

— правила защиты персональных данных;

— назначение различных позитивных ресурсов в сети Интернет для образования и в профессиях будущего.

Выпускник научится применять на практике:

— правила цифровой гигиены для использования средств защиты персональных данных (формировать и использовать пароль, использовать код защиты персонального устройства, регистрироваться на сайтах без распространения личных данных);

— компетенции медиаинформационной грамотности при работе с информацией в сети Интернет, критическое и избирательное отношение к источникам информации;

— компетенции компьютерной грамотности по защите персональных устройств от вредоносных программ, использованию антивирусных программных средств, лицензионного программного обеспечения;

— информационно-коммуникативные компетенции по соблюдению этических и правовых норм взаимодействия в социальной сети или в мессенджере, умение правильно вести себя в проблемной ситуации (оскорбления, угрозы, предложения, агрессия, вымогательство, ложная информация и др.), отключаться от нежелательных контактов, действовать согласно правовым нормам в сфере информационной безопасности (защиты информации).

Выпускник освоит нормы культуры информационной безопасности в системе универсальных учебных действий для самостоятельного использования в учебно-познавательной и досуговой деятельности позитивного Интернета и средств электронного обучения с соблюдением правил информационной безопасности.

Для выявления достижения планируемых результатов обучения используются диагностические тесты и опросы, проектные работы и конкурсы по информационной безопасности.

ТЕМАТИЧЕСКОЕ ПЛАНИРОВАНИЕ КУРСА «ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ»

№ п/п	Наименование модулей	Кол-во часов		
		7 класс	8 класс	9 класс
1	Общие сведения о безопасности ПК и Интернета	5	5	11
2	Техника безопасности и экология.	5	2	3
3	Проблемы Интернет-зависимости	2	3	2
4	Методы обеспечения безопасности ПК и Интернета. Вирусы и антивирусы	8	16	7
5	Мошеннические действия в Интернете. Киберпреступления	2	4	7
6	Сетевой этикет. Психология и сеть	10	1	1
7	Правовые аспекты защиты киберпространства	2	3	3
	Всего часов:	**34**	**34**	**34**

Поурочное планирование

7 класс (34 часа)

№ урока	Тема	Кол-во часов
	Общие сведения о безопасности ПК и Интернета	**5**
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 (ГИС). Глобальные информационные Сети по стихийным бедствиям.	1
	Техника безопасности и экология.	**5**
6	Компьютер и мобильные устройства в чрезвычайных ситуациях. 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.	1
9	Первая помощь при проблемах в интернете (службы помощи).	1
10	Воздействие радиоволн на здоровье и окружающую среду (Wi-Fi, Bluetooth, GSM).	1
	Проблемы Интернет-зависимости.	**2**
11	Виды Интернет-зависимости.	1
12	Компьютер и зрение.	1
	Методы обеспечения безопасности ПК и Интернета. Вирусы и антивирусы.	**8**
13	Как распространяются вирусы.	1
14	Источники и причины заражения.	1
15	Скорая компьютерная помощь. Признаки заражения компьютера.	1
16	Что такое антивирусная защита. Как лечить компьютер.	1
17	Защита мобильных устройств.	1
18	Как защитить данные от потерь. Копирование и восстановление. Всегда ли можно спасти свои данные.	1
19	Защита файлов. Что такое право доступа.	1
20	Защита детей в социальных сетях. ПО для родителей. Ограничение времени нахождения в сети.	1
	Мошеннические действия в Интернете. Киберпреступления.	**2**
21	Опасности мобильной связи. Предложения по установке вредоносных приложений. Мошеннические СМС.	1
22	Прослушивание разговоров. Определение местоположения телефона.	1
	Сетевой этикет. Психология и сеть.	**10**
23	Что такое личные данные. Все, что выложено в Интернет, может стать известно всем.	1
24	«Лишняя информация» о себе и других в Интернете. Какая информация принадлежит вам.	1
25	Анонимность в сети.	1
26	Что такое этикет. Виды этикета (личный, деловой, письменный, дискуссионный и пр.). Различия этикета в разных странах.	1
27	Как появился нетикет, что это такое. Общие правила сетевого этикета.	1
28	Личное общение и общение в группе – чем они отличаются (чаты, форумы, службы мгновенных сообщений).	1
29	Этика дискуссий. Взаимное уважение при интернет-общении.	1
30	Этикет и безопасность. Эмоции в сети, их выражение.	1
31	Реальная и виртуальная личность, реальные встречи с виртуальными знакомыми и их опасность, угрозы и оскорбления – чем это может закончиться.	1
32	Если вы стали жертвой компьютерной агрессии: службы помощи.	1
	Правовые аспекты защиты киберпространства.	**2**

33	Собственность в Интернете. Авторское право. Интеллектуальная собственность. Платная и бесплатная информация.	1
34	Обобщение материала курса. Игра-квест «Знатоки кибербезопасности».	1

8 класс (34 часа)

№ урока	Тема	Кол-во часов
	Общие сведения о безопасности ПК и Интернета	**5**
1	Информационная безопасность	1
2	Защита персональных данных, почему она нужна. Категории персональных данных. Биометрические персональные данные.	1
3	Источники данных в Интернете: почта, сервисы обмена файлами и др. Хранение данных в Интернете.	1
4	Возможности и проблемы социальных сетей.	1
5	Безопасный профиль в социальных сетях. Составление сети контактов.	1
	Техника безопасности и экология.	**2**
6	Комплекс упражнений при работе за компьютером.	1
7	Воздействие на зрение ЭЛТ, жидкокристаллических, светодиодных, монохромных мониторов.	1
	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.	1
9	Киберкультура (массовая культура в сети) и личность.	1
10	Психологическое воздействие информации на человека. Управление личностью через сеть.	1
	Методы обеспечения безопасности ПК и Интернета. Вирусы и антивирусы.	**16**
11	Защита файлов. Права пользователей.	1
12	Защита при загрузке и выключении компьютера.	1
13	Безопасность при скачивании файлов.	1
14	Безопасность при просмотре фильмов онлайн.	1
15	Защита программ и данных от несанкционированного копирования. Организационные, юридические, программные и программно-аппаратные меры защиты.	1
16	Защита программ и данных с помощью паролей, программных и электронных ключей, серийных номеров, переноса в онлайн и т.п. Неперемещаемые программы.	1
17	Методы защиты фото и видеоматериалов от копирования в сети.	1
18	Защита от копирования контента сайта.	1
19	Как развивались вирусы.	1
20	Могут ли вирусы воздействовать на аппаратуру ПК.	1
21	Как вирусы воздействуют на файлы.	1
22	Проверка на наличие вирусов. Сканеры и др.	1

23	Может ли вирус воздействовать на рабочий стол.	1
24	Источники заражения ПК.	1
25	Антивирусное ПО, виды и назначение.	1
26	Методы защиты от вирусов. Как распознаются вирусы.	1
	Мошеннические действия в Интернете. Киберпреступления.	**4**
27	Утечка и обнародование личных данных.	1
28	Подбор и перехват паролей. Взломы аккаунтов в социальных сетях.	1
29	Виды мошенничества в Интернете. Фишинг (фарминг).	1
30	Азартные игры. Онлайн-казино. Букмекерские конторы. Предложения для «инвестирования» денег. Выигрыш в лотерею.	1
	Сетевой этикет. Психология и сеть.	**1**
31	Психологическая обстановка в Интернете: грифинг, кибербуллинг, кибер-моббинг, троллинг, буллицид.	1
	Правовые аспекты защиты киберпространства.	**3**
32	Защита прав потребителей при использовании услуг Интернет.	1
33	Защита прав потребителей услуг провайдера.	1
34	Обобщение материала курса. Игра-квест «Знатоки кибербезопасности».	1

9 класс (34 часа)

№ 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.	1
2	Компьютерная и информационная безопасность, обнаружение проблем сети, восстановление параметров систем, средства защиты от несанкционированного доступа к данным, криптографическая защита информации.	1
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.	1
4	Организационно-технические меры защиты информационной среды. Системы охранной сигнализации, видеонаблюдение, контроль и управление доступом, средства уничтожения информации, средства резервного копирования и восстановления.	1
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».	1
6	Признаки нарушения целостности программ и данных. Способы нарушения целостности информации. Признаки и способы нарушения конфиденциальности. Признаки и способы нарушения доступности информации.	1
7	Безопасность мобильных устройств в информационных системах.	1

	Источники заражения мобильных устройств (веб-ресурсы, магазины приложений, ботнеты).	
8	Угрозы безопасности в сетях WiFi. Методы защиты сетей WiFi.	1
9	Угрозы информации (техногенные, случайные и преднамеренные; природные). Неосторожность пользователя как одна из угроз для информационной безопасности.	1
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.	1
11	Киберугрозы Интернета (кибервойны, манипулирование людьми, зависимость, вирусные атаки, отсутствие приватности).	1
	Техника безопасности и экология.	**3**
12	Кибератаки на инфраструктуру.	1
13	Компьютер в режиме труда и отдыха. Информационная перегрузка.	1
14	Влияние компьютера на репродуктивную систему.	1
	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.	1
16	Типы интернет-зависимости (пристрастие к работе с компьютером, к навигации и поиску информации, игромания и электронные покупки, зависимость от сетевого общения, сексуальные зависимости).	1
	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.	1
18	Проверка подлинности (аутентификация) в Интернете.	1
19	Меры безопасности для пользователя WiFi. Настройка безопасности.	1
20	Вирусы для мобильных устройств (мобильные банкеры и др.).	1
21	Настройка компьютера для безопасной работы.	1
22	Ошибки пользователя (установка нескольких антивирусов, установка слишком большого числа программ, отсутствие резервного копирования и т.п.).	1
23	Меры личной безопасности при сетевом общении. Настройки приватности в социальных сетях.	1
	Мошеннические действия в Интернете. Киберпреступления.	**7**
24	Мошеннические действия в сети. Предложения о разблокировании программ (блокировщики windows). Ложные антивирусы.	1
25	Подмена страниц в интернете (сайты-клоны). Фальшивые файлообменники.	1
26	Мошеннические действия в сети. Сбор «пожертвований» на благотворительность. «Легкий заработок» в Интернете. Пирамиды.	1
27	Что такое электронный кошелек – удобства и проблемы безопасности. «Обменники» для электронных денег.	1
28	Мошенничество при распространении «бесплатного» ПО. Продажа	1

	«обучающих курсов» для бизнеса.	
29	Платные предложения работы. Платный просмотр видеоматериалов.	1
30	Технологии манипулирования в Интернете.	1
	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.	1
	Правовые аспекты защиты киберпространства.	**3**
32	Как расследуются преступления в сети.	1
33	Ответственность за интернет-мошенничество.	1
34	Обобщение материала курса. Игра-квест «Знатоки кибербезопасности».	1