

МИНИСТЕРСТВО ПРОСВЕЩЕНИЯ РОССИЙСКОЙ ФЕДЕРАЦИИ

**Управление образования
администрации города Невинномысска**

**Муниципальное бюджетное общеобразовательное учреждение средняя
общеобразовательная школа № 2 города Невинномысска имени
летчика-космонавта, Героя Российской Федерации
Олега Ивановича Скрипочки**

МБОУ СОШ № 2 г. Невинномысска имени О.И. Скрипочки

РАССМОТРЕНО

Руководитель
ШМО

С.А.Савельева

Протокол № 1
от « 28 » августа 2024 г.

СОГЛАСОВАНО

Заместитель директора
по УВР

С.С.Мусаева

Протокол № 1
от « 28 » августа 2024 г.

УТВЕРЖДЕНО

Директор МБОУ СОШ № 2
г. Невинномысска
имени О.И. Скрипочки

М.А. Маланин

Приказ № 96-о/д
от « 28 » августа 2024 г.

РАБОЧАЯ ПРОГРАММА

(ID 45101093)

учебного предмета «Информационная безопасность»

для обучающихся 5 – 9 классов

г. Невинномысск, 2024г.

ПОЯСНИТЕЛЬНАЯ ЗАПИСКА

ОБЩАЯ ХАРАКТЕРИСТИКА УЧЕБНОГО ПРЕДМЕТА "Информационная безопасность"

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.

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 теньевые, закрытые субкультуры, несущие угрозу здоровью и даже жизни ребенка.

Раздел программы курса для 5—6 классов отражает практические вопросы и жизненные проблемы:

- негативный и позитивный Интернет, цифровизация профессий;
- культура организации компьютерного досуга и профилактика игромании;
- мошенники в сети Интернет;

- агрессия в Интернете;
- сетевой этикет;
- навязчивые предложения;
- правила регистрации в электронных ресурсах и защита личных данных.

Раздел программы курса для 7—9 классов отражает особенности современного цифрового мира как киберпространства, насыщенного сетевыми сервисами и интернет-коммуникациями, доступными детям, новыми сервисами и устройствами с искусственным интеллектом (умные вещи, Интернет вещей), в том числе несущими в себе угрозы:

- закрытые сетевые сообщества неизвестного толка, опасные группы, негативные контакты;
- навязчивые интернет-ресурсы (спам, реклама, азартные игровые сервисы);
- сайты, содержащие негативный и агрессивный контент, в том числе противоправные материалы, влекущие ответственность по законам Российской Федерации;
- сетевые средства вмешательства в личное информационное пространство на персональных устройствах, работающих в Интернете;
- использование электронных сервисов, социальных/банковских карт, имеющих персональные настройки доступа к ним.

Отражение потребностей цифрового мира в современной цифровой грамотности и новых профессиональных качествах современного человека востребовано в жизни и учебе школьников и несет в себе актуальные запросы для выпускника основного общего образования в его дальнейшей жизни и профессиональном выборе с обязательным использованием требований информационной безопасности:

- профориентация в мире профессий будущего, знакомство с профессиями в сфере информационной безопасности;
- популяризация электронных средств и ресурсов обучения;

- развитие кругозора о полезных интернет-ресурсах;
- получение представлений о цифровых технологиях для улучшения качества жизни;
- навыки обдуманного поведения при поиске информации в сети Интернет, критический анализ полученной информации, умение работать с информацией избирательно и ответственно.

ЦЕЛИ ИЗУЧЕНИЯ УЧЕБНОГО ПРЕДМЕТА "Информационная безопасность"

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 ПРЕДМЕТА "Информационная безопасность" В УЧЕБНОМ ПЛАНЕ

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 их возрастных особенностей. Программа курса ориентирована на включение в контекст обучения и воспитания новых видов информационных угроз и средств противодействия им. Программа курса представлена двумя разделами по возрастным группам: для 5—6 классов и 7—9 классов. Реализация программы учебного курса возможна в разных формах:

- как дополнительные модули обучения в интеграции с предметами «Информатика» и (или) «ОБЖ» для двух возрастных групп: 5—6 и 7—9 классов (34 учебных часа для каждой возрастной группы);
- в рамках отдельного учебного курса «Информационная безопасность» для внеурочной деятельности по выбору из объема часов, формируемых самостоятельно образовательной организацией;
- в рамках часов, предусмотренных по программе воспитания (социализации) в образовательной организации для разных уровней общего образования.

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.

СОДЕРЖАНИЕ УЧЕБНОГО ПРЕДМЕТА "Информационная безопасность"

Содержание учебного курса «Информационная безопасность» для разных возрастных модулей программы складывается из двух линий:

- 1) Информационное общество и информационная культура.
- 2) Информационное пространство и правила информационной безопасности.

5 КЛАСС

Линия «Информационное общество и информационная культура»

Модуль 1. Информационное общество.

- 1. Информационное общество.

История создания сети Интернет.

Что такое Всемирная паутина?

1.2. Интернет как глобальная компьютерная сеть.

Как стать пользователем Интернета. Опасности для пользователей Интернета.

Сайты, электронные сервисы.

1.3. Угрозы в сети Интернет.

Защита личных данных в сети Интернет.

1.4. Сетевой этикет.

Коллекции сайтов для детей. Электронные музеи.

Линия «Информационное пространство и правила информационной безопасности»

Модуль 2. Правила пользователей сети Интернет.

2.1. Работа с СМС, электронной почтой, видеосервисами, в чатах и социальных сетях. Что такое информационная безопасность.

2.2. Защита от вредоносных программ и нежелательных рассылок, от негативных сообщений, защита своих устройств от внешнего вторжения.

2.3. Общение в социальной сети, работа с поисковыми системами и анализ информации, ответственность за распространение ложной и негативной информации, защита от нежелательных сообщений и контактов, вызов экстренной помощи.

2.4. Использование полезных ресурсов в сети Интернет, работа в сети Интернет для людей с особыми потребностями.

6 КЛАСС

Линия «Информационное общество и информационная культура»

Модуль 1. Информационное общество.

- 1. Информационное общество.

История создания сети Интернет.

Что такое Всемирная паутина?

1.2. Интернет как глобальная компьютерная сеть.

Как стать пользователем Интернета. Опасности для пользователей Интернета.

Сайты, электронные сервисы.

1.3. Угрозы в сети Интернет.

Защита личных данных в сети Интернет.

1.4. Сетевой этикет.

Коллекции сайтов для детей. Электронные музеи.

Линия «Информационное пространство и правила информационной безопасности»

Модуль 2. Правила пользователей сети Интернет.

2.1. Работа с СМС, электронной почтой, видеосервисами, в чатах и социальных сетях. Что такое информационная безопасность.

2.2. Защита от вредоносных программ и нежелательных рассылок, от негативных сообщений, защита своих устройств от внешнего вторжения.

2.3. Общение в социальной сети, работа с поисковыми системами и анализ информации, ответственность за распространение ложной и

негативной информации, защита от нежелательных сообщений и контактов, вызов экстренной помощи.

2.4. Использование полезных ресурсов в сети Интернет, работа в сети Интернет для людей с особыми потребностями.

7 КЛАСС

Линия «Информационное общество и информационная культура»

Модуль 1. Современное информационное пространство и искусственный интеллект. 1.1. Киберпространство. Кибермиры. Киберфизическая система.

1.2. Киберобщество. Киберденьги. Кибермошенничество.

Модуль 2. Современная информационная культура.

2.1. Киберкультура. От книги к гипертексту. Киберкнига. Киберискусство.

2.2. Социальная инженерия. Классификация угроз социальной инженерии.

2.3. Новые профессии в киберобществе. Цифровизация профессий.

Линия «Информационное пространство и правила информационной безопасности»

Модуль 3. Угрозы информационной безопасности.

3.1. Киберугрозы. Кибервойны. Киберпреступность.

Уязвимости кибербезопасность.

Запрещенные и нежелательные сайты.

3.2. Защита от вредоносных программ и информационных атак.

3.3. Практика электронного обучения в сфере информационной безопасности.

8 КЛАСС

Линия «Информационное общество и информационная культура»

Модуль 1. Современное информационное пространство и искусственный интеллект. 1.1. Киберпространство. Кибермиры. Киберфизическая система.

1.2. Киберобщество. Киберденьги. Кибермошенничество.

Модуль 2. Современная информационная культура.

2.1. Киберкультура. От книги к гипертексту. Киберкнига. Киберискусство.

2.2. Социальная инженерия. Классификация угроз социальной инженерии.

2.3. Новые профессии в киберобществе. Цифровизация профессий.

Линия «Информационное пространство и правила информационной безопасности»

Модуль 3. Угрозы информационной безопасности.

3.1. Киберугрозы. Кибервойны. Киберпреступность.

Уязвимости кибербезопасность.

Запрещенные и нежелательные сайты.

3.2. Защита от вредоносных программ и информационных атак.

3.3. Практика электронного обучения в сфере информационной безопасности.

9 КЛАСС

Линия «Информационное общество и информационная культура»

Модуль 1. Современное информационное пространство и искусственный интеллект. 1.1. Киберпространство. Кибермиры.

Киберфизическая система.

1.2. Киберобщество. Киберденьги. Кибермошенничество.

Модуль 2. Современная информационная культура.

2.1. Киберкультура. От книги к гипертексту. Киберкнига. Киберискусство.

2.2. Социальная инженерия. Классификация угроз социальной инженерии.

2.3. Новые профессии в киберобществе. Цифровизация профессий.

Линия «Информационное пространство и правила информационной безопасности»

Модуль 3. Угрозы информационной безопасности.

3.1. Киберугрозы. Кибервойны. Киберпреступность.

Уязвимости кибербезопасность.

Запрещенные и нежелательные сайты.

3.2. Защита от вредоносных программ и информационных атак.

3.3. Практика электронного обучения в сфере информационной безопасности.

ПЛАНИРУЕМЫЕ ОБРАЗОВАТЕЛЬНЫЕ РЕЗУЛЬТАТЫ

ЛИЧНОСТНЫЕ РЕЗУЛЬТАТЫ

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 личного 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.

МЕТАПРЕДМЕТНЫЕ РЕЗУЛЬТАТЫ

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.

ПРЕДМЕТНЫЕ РЕЗУЛЬТАТЫ

5 КЛАСС

Планируется достижение *предметных результатов*, актуальных для курса информационной безопасности в интеграции с предметами «Информатика» и (или) «ОБЖ» для 5—6 и 7—9 классов.

Линия «Информационное общество и информационная культура»:

- 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.

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 рекомендуется использовать диагностические тесты и опросы, проектные работы и конкурсы по информационной безопасности в образовательных организациях.

6 КЛАСС

Планируется достижение *предметных результатов*, актуальных для курса информационной безопасности в интеграции с предметами «Информатика» и (или) «ОБЖ» для 5—6 и 7—9 классов.

Линия «Информационное общество и информационная культура»:

— 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.

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 рекомендуется использовать диагностические тесты и опросы, проектные работы и конкурсы по информационной безопасности в образовательных организациях.

7 КЛАСС

Линия «Информационное пространство и правила информационной безопасности»:

- 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.

8 КЛАСС

Линия «Информационное пространство и правила информационной безопасности»:

— 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.

9 КЛАСС

Линия «Информационное пространство и правила информационной безопасности»:

— 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.

**ТЕМАТИЧЕСКОЕ ПЛАНИРОВАНИЕ
5 КЛАСС**

№ п/п	Наименование разделов и тем программы	Количество часов			Электронные (цифровые) образовательные ресурсы
		Всего	Контрольные работы	Практические работы	
1	Введение	1	0	0	
2	Раздел 1. Что нужно знать? Пространство Интернета на планете Земля	33	2	8	
ОБЩЕЕ КОЛИЧЕСТВО ЧАСОВ ПО ПРОГРАММЕ		34	2	8	

6 КЛАСС

№ п/п	Наименование разделов и тем программы	Количество часов			Электронные (цифровые) образовательные ресурсы
		Всего	Контрольные работы	Практические работы	
1	Введение	1	0	0	
2	Раздел 2. Что нужно уметь? Правила для пользователей Сети Интернет	33	2	8	
ОБЩЕЕ КОЛИЧЕСТВО ЧАСОВ ПО ПРОГРАММЕ		34	2	8	

7 КЛАСС

№ п/п	Наименование разделов и тем программы	Количество часов			Электронные (цифровые) образовательные ресурсы
		Всего	Контрольные работы	Практические работы	
1	Введение	1	0	0	
2	Раздел "Безопасность общения"	33	0	10	
ОБЩЕЕ КОЛИЧЕСТВО ЧАСОВ ПО ПРОГРАММЕ		34	0	10	

8 КЛАСС

№ п/п	Наименование разделов и тем программы	Количество часов			Электронные (цифровые) образовательные ресурсы
		Всего	Контрольные работы	Практические работы	
1	Введение	1	0	0	
2	Безопасность устройств	33	0	10	
ОБЩЕЕ КОЛИЧЕСТВО ЧАСОВ ПО ПРОГРАММЕ		34	0	10	

9 КЛАСС

№ п/п	Наименование разделов и тем программы	Количество часов			Электронные (цифровые) образовательные ресурсы
		Всего	Контрольные работы	Практические работы	
1	Введение	1	0	0	
2	Безопасность информации	33	0	13	
ОБЩЕЕ КОЛИЧЕСТВО ЧАСОВ ПО ПРОГРАММЕ		34	0	13	

ПОУРОЧНОЕ ПЛАНИРОВАНИЕ
5 КЛАСС

№ п/п	Тема урока	Количество часов			Дата изучения	Электронные цифровые образовательные ресурсы
		Всего	Контрольные работы	Практические работы		
1	Техника безопасности в кабинете информатики и организация рабочего места	1	0	0		
2	Что нужно знать? Пространство интернета на планете Земля	1	0	0		https://uchitelya.com/informatika/17356-prezentaciya-bezopasnost-v-internete-5-klass.html
3	Угрозы Интернета для детей	1	0	0		https://nsportal.ru/nachalnaya-shkola/informatika/2018/02/12/prezentatsiya-ugrozy-dlya-detey-v-internete
4	Мировой опыт защиты детей в Интернете	1	0	0		https://nsportal.ru/nachalnaya-shkola/informatika/2018/02/12/prezentatsiya-ugrozy-dlya-detey-v-internete
5	История создания сети Интернет.	1	0	0		https://nsportal.ru/shkola/informatika-i-ikt/library/2021/08/26/istoriya-interneta
6	Практическая работа № 1 "Где находится Интернет"	1	0	1		
7	Что такое Всемирная	1	0	0		

	паутина					
8	Практическая работа №2 «Ищем информацию в сети интернет».	1	0	1		
9	Путешествие по сети Интернет: сайты и электронные сервисы	1	0	0		
10	Практическая работа № 3 "Знакомство с детскими с соц сетями"	1	0	1		
11	Как стать пользователем Интернета	1	0	0		
12	Практическая работа № 4 "Я пользователь сети Интернет"	1	0	1		
13	Опасности для пользователей Интернета	1	0	0		
14	Контрольная работа № 1 "Интернет"	1	1	0		
15	Что такое кибератака	1	0	0		https://videouroki.net/razrabotki/kiberataki-i-kiberterrorizm.html
16	Что такое кибербуллинг	1	0	0		https://multiurok.ru/index.php/files/prezentatsiia-po-teme-kiberbulling.html

17	Практическая работа № 5 "Антивирусы"	1	0	1		
18	Что такое информационная безопасность	1	0	0		
19	Практическая работа № 6 "Личная памятка безопасности при работе в сети Интернет"	1	0	1		
20	Законы о защите личных данных в Интернете	1	0	0		
21	Законы о защите личных данных в Интернете	1	0	0		
22	Персональные данные. Знакомство с сайтами	1	0	0		
23	Игра «Приключения робота Каспера»	1	0	0		
24	Сетевой этикет	1	0	0		
25	Знакомство с сайтом «Защита детей»	1	0	0		
26	Практическая работа № 7 «Правила поведения в	1	0	1		

	коллективе»					
27	Коллекция сайтов для детей	1	0	0		
28	Путешествие по ресурсам сайта «Вебландия»	1	0	0		
29	Электронные музеи	1	0	0		
30	Электронные музеи	1	0	0		
31	Практическая работа в форме промежуточной аттестации	1	0	0		
32	Повторение	1	0	0		
33	Контрольная работа № 2 «Информационная безопасность»	1	1	0		
34	Повторение	1	0	0		
ОБЩЕЕ КОЛИЧЕСТВО ЧАСОВ ПО ПРОГРАММЕ		34	2	7		

6 КЛАСС

№ п/п	Тема урока	Количество часов			Дата изучения	Электронные цифровые образовательные ресурсы
		Всего	Контрольные работы	Практические работы		
1	Техника безопасности в кабинете информатики и организация рабочего места.	1	0	0		
2	Правила работы с СМС	1	0	0		https://uchitelya.com/pedagogika/142150-prezentaciya-obuchenie-novoy-forme-obscheniya-sms.html
3	Получение подозрительных СМС сообщений	1	0	0		https://uchitelya.com/pedagogika/142150-prezentaciya-obuchenie-novoy-forme-obscheniya-sms.html
4	Правила работы с электронной почтой	1	0	0		https://multiurok.ru/files/prezentatsiia-po-teme-rabota-s-elektronnoi-pochtoi.html
5	Анализ сайтов для выбора при создании электронной почты	1	0	0		https://multiurok.ru/files/prezentatsiia-po-teme-rabota-s-elektronnoi-pochtoi.html
6	Практическая работа № 1. Правила отправки и получения электронных писем	1	0	1		
7	Правила работы с видеосервисами	1	0	0		
8	Практическая работа № 2	1	0	1		
9	Практическая работа № 3	1	0	1		

10	Правила работы в социальных сетях	1	0	0		
11	.Анализ социальных сетей	1	0	0		
12	. Практическая работа № 5 «Смайлы»	1	0	1		
13	Правила защиты от вирусов, спама, рекламы и рассылок. Практическая работа № 6 «Памятка»	1	0	1		
14	Контрольная работа № 1 "Пользователи сети Интернет"	1	1	0		
15	Правила защиты.	1	0	0		
16	Настройка защиты от негативных сообщений	1	0	0		
17	Практическая работа № 7 «Буклет»	1	0	1		
18	Этикет	1	0	0		
19	Переписка с друзьями, с родственниками.	1	0	0		
20	Правила работы с поисковыми системами и анализ информации	1	0	0		
21	Правила работы с поисковыми системами и анализ информации	1	0	0		

22	Правила ответственности за распространение ложной и негативной информации	1	0	0		
23	Правила ответственности за распространение ложной и негативной информации	1	0	0		
24	Правила защиты от нежелательных сообщений и контактов	1	0	0		
25	Правила вызова экстренной помощи.	1	0	0		
26	Правила защиты от внешнего вторжения.	1	0	0		
27	Правила выбора полезных ресурсов в Интернете.	1	0	0		
28	Практическая работа № 8 «Знакомство с полезными ресурсами»	1	0	1		
29	Средства работы в Интернете для людей с особыми потребностями	1	0	0		
30	Практическая работа № 9 «Средства работы в Интернете для людей с особыми потребностями»	1	0	1		

31	Практическая работа в форме промежуточной аттестации	1	0	0		
32	Повторение	1	0	0		
33	Контрольная работа № 2 «Информационная безопасность»	1	1	0		
34	Повторение	1	0	0		
ОБЩЕЕ КОЛИЧЕСТВО ЧАСОВ ПО ПРОГРАММЕ		34	2	8		

7 КЛАСС

№ п/п	Тема урока	Количество часов			Дата изучения	Электронные цифровые образовательные ресурсы
		Всего	Контрольные работы	Практические работы		
1	Техника безопасности в кабинете информатики и организация рабочего места.	1	0	0		
2	Общение в социальных сетях.	1	0	0		
3	Обсуждение тем индивидуальных проектов проектов	1	0	0		
4	Социальная сеть. История социальных сетей.	1	0	0		
5	Мессенджеры. Назначение социальных сетей и мессенджеров.	1	0	0		
6	Пользовательский контент	1	0	0		
7	Правила добавления друзей с соцсетях. Профиль пользователя.	1	0	0		
8	Анонимные социальные сети.	1	0	0		
9	Пароли для аккаунтов социальных сетей.	1	0	0		
10	Пароли для аккаунтов социальных сетей.	1	0	1		
11	Безопасный вход в аккаунт.	1	0	0		
12	Безопасный вход в аккаунт.	1	0	1		
13	Настройки конфиденциальность в социальных сетях.	1	0	0		

14	Настройки конфиденциальность в социальных сетях.	1	0	1		
15	Публикация информации в социальных сетях.	1	0	0		
16	Публикация информации в социальных сетях.	1	0	1		
17	Персональные данные.	1	0	0		
18	Персональные данные.	1	0	1		
19	Кибербуллинг.	1	0	0		
20	Кибербуллинг.	1	0	0		
21	Кибербуллинг.	1	0	0		
22	Публичные аккаунты.	1	0	0		
23	Публичные аккаунты.	1	0	1		
24	Фишинг	1	0	0		
25	Фишинг	1	0	0		
26	Тест по теме «Безопасность общения»	1	0	0		
27	Работа над индивидуальными и групповыми проектами.	1	0	1		
28	Работа над индивидуальными и групповыми проектами.	1	0	1		
29	Работа над индивидуальными и групповыми проектами.	1	0	1		
30	Работа над индивидуальными и групповыми проектами.	1	0	1		
31	Защита индивидуальных и групповых проектов.	1	0	0		
32	Защита индивидуальных и групповых	1	0	0		

	проектов.					
33	Повторение	1	0	0		
34	Повторение	1	0	0		
ОБЩЕЕ КОЛИЧЕСТВО ЧАСОВ ПО ПРОГРАММЕ		34	0	10		

8 КЛАСС

№ п/ п	Тема урока	Количество часов			Дата изучени я	Электронные цифровые образовательные ресурсы
		Всег о	Контрольны е работы	Практически е работы		
1	Техника безопасности в кабинете информатики и организация рабочего места.	1	0	0		
2	Что такое вредоносный код	1	0	0		https://nsportal.ru/ap/library/drugoe/2017/02/28/prezentatsiya-vredonosnye-programmy
3	Что такое вредоносный код	1	0	0		https://nsportal.ru/ap/library/drugoe/2017/02/28/prezentatsiya-vredonosnye-programmy
4	Распространение вредоносного кода.	1	0	0		https://nsportal.ru/ap/library/drugoe/2017/02/28/prezentatsiya-vredonosnye-programmy
5	Распространение вредоносного кода.	1	0	0		https://nsportal.ru/ap/library/drugoe/2017/02/28/prezentatsiya-vredonosnye-programmy
6	Способы выявления вредоносных кодов.	1	0	0		https://nsportal.ru/ap/library/drugoe/2017/02/28/prezentatsiya-vredonosnye-programmy
7	Способы выявления вредоносных	1	0	1		

	кодов.					
8	Действия при обнаружении вредоносных кодов.	1	0	1		
9	Методы защиты от вредоносных программ.	1	0	0		https://nsportal.ru/ap/library/drugoe/2017/02/28/prezentatsiya-vredonosnye-programmy
10	Методы защиты от вредоносных программ.	1	0	1		
11	Антивирусные программы и их характеристики.	1	0	0		https://nsportal.ru/npo-spo/informatika-i-vychislitel'naya-tehnika/library/2013/12/04/prezentatsiya-na-temu-antivirusnye
12	Антивирусные программы и их характеристики.	1	0	0		https://nsportal.ru/npo-spo/informatika-i-vychislitel'naya-tehnika/library/2013/12/04/prezentatsiya-na-temu-antivirusnye
13	Антивирусные программы и их характеристики.	1	0	1		
14	Распространение вредоносного кода для мобильных устройств.	1	0	0		
15	Распространение вредоносного кода для	1	0	1		

	мобильных устройств.					
16	Особенности безопасного Хранения данных на USB-флеш носителях	1	0	0		
17	Особенности безопасного Хранения данных на USB-флеш носителях	1	0	1		
18	Обобщение материала	1	0	0		
19	Подготовка к тесту "Безопасность устройств"	1	0	0		
20	Тест по теме «Безопасность устройств»	1	0	0		
21	Анализ выполнения теста	1	0	0		
22	Обсуждение тем индивидуальных и групповых проектов	1	0	0		

23	Обсуждение тем индивидуальных и групповых проектов	1	0	0		
24	Работа над индивидуальным и и групповыми проектами.	1	0	1		
25	Работа над индивидуальным и и групповыми проектами	1	0	1		
26	Работа над индивидуальным и и групповыми проектами	1	0	1		
27	Работа над индивидуальным и и групповыми проектами	1	0	1		
28	Защита индивидуальных и групповых проектов.	1	0	0		
29	Защита индивидуальных и групповых проектов.	1	0	0		
30	Защита	1	0	0		

	индивидуальных и групповых проектов.					
31	Повторение	1	0	0		
32	Повторение	1	0	0		
33	Повторение	1	0	0		
34	Повторение	1	0	0		
ОБЩЕЕ КОЛИЧЕСТВО ЧАСОВ ПО ПРОГРАММЕ		34	0	10		

9 КЛАСС

№ п/п	Тема урока	Количество часов			Дата изучения	Электронные цифровые образовательные ресурсы
		Всего	Контрольные работы	Практические работы		
1	Техника безопасности в кабинете информатики и организация рабочего места.	1				
2	Правовое обеспечение информационной безопасности	1				
3	Основные угрозы информационной безопасности	1				
4	Основные угрозы информационной безопасности	1		1		
5	Что такое персональные данные?	1				
6	Социальная инженерия: распознать и избежать.	1				https://infourok.ru/informacionnaya-bezопасnost-tema-socialnaya-inzheneriya-9-klass-5214109.html
7	Социальная инженерия: распознать и избежать.	1		1		
8	Правила безопасность при виртуальных контактах.	1		1		
9	Ложная информация в Интернете.	1				

10	Ложная информация в Интернете.	1		1		
11	Безопасность при использовании платежных карт в Интернете.	1				
12	Правила совершения онлайн покупок	1				
13	Беспроводная технология связи	1				https://infourok.ru/prezentaciya-po-informatike-na-temu-besprovodnie-seti-1739279.html
14	Беспроводная технология связи	1		1		
15	Уязвимость Wi-Fi — соединений.	1		1		https://infourok.ru/prezentaciya-po-informatike-na-temu-besprovodnie-seti-1739279.html
16	Публичные и непубличные сети.	1				https://infourok.ru/prezentaciya-po-informatike-na-temu-besprovodnie-seti-1739279.html
17	Правила работы в публичных сетях.	1				
18	Резервное копирование данных.	1		1		
19	Безопасность личной информации	1				
20	Что такое цифровая подпись и безопасность ее использования	1				
21	Спам в интернет сетях.	1		1		
22	Родительский контроль.	1		1		

23	Тест по теме «Безопасность информации»	1				
24	Обсуждение тем индивидуальных и групповых проектов	1				
25	Обсуждение тем индивидуальных и групповых проектов	1				
26	Работа над индивидуальными и групповыми проектами.	1		1		
27	Работа над индивидуальными и групповыми проектами.	1		1		
28	Работа над индивидуальными и групповыми проектами.	1		1		
29	Работа над индивидуальными и групповыми проектами.	1		1		
30	Защита индивидуальных и групповых проектов.	1				
31	Защита индивидуальных и групповых проектов.	1				
32	Защита индивидуальных и групповых проектов.	1				
33	Повторение	1				
34	Повторение	1				

ОБЩЕЕ КОЛИЧЕСТВО ЧАСОВ ПО ПРОГРАММЕ	34	0	13	
--	----	---	----	--

Список литературы и интернет-ресурсов

1. Бабаш А.В. Информационная безопасность: Лабораторный практикум / А.В. Бабаш, Е.К. Баранова, Ю.Н. Мельников. – М.: КноРус, 2019 – 432 с
2. Вехов В. Б. Компьютерные преступления: способы совершения и раскрытия / В.Б. Вехов; Под ред. акад. Б.П. Смагоринского. – М.: Право и закон, 2014 – 182 с.
3. Громов Ю.Ю. Информационная безопасность и защита информации: Учебное пособие / Ю.Ю. Громов, В.О. Драчев, О.Г. Иванова. – Ст. Оскол: ТНТ, 2017 – 384 с.
- . Дети в информационном обществе <http://detionline.com/journal/about>
5. Ефимова Л.Л. Информационная безопасность детей. Российский и зарубежный опыт: Монография / Л.Л. Ефимова, С.А. Кочерга. – М.: ЮНИТИДАНА, 2016 – 239 с.
6. Запечников С.В. Информационная безопасность открытых систем. В 2-х т. Т.2 – Средства защиты в сетях / С.В. Запечников, Н.Г. Милославская, А.И. Толстой, Д.В. Ушаков. – М.: ГЛТ, 2018 – 558 с.
7. Защита детей by Kaspersky // <https://kids.kaspersky.ru/>
8. Кузнецова А.В. Искусственный интеллект и информационная безопасность общества / А.В. Кузнецова, С.И. Самыгин, М.В. Радионов. – М.: Русайнс, 2017 – 64 с.
9. Наместникова М.С. Информационная безопасность, или На расстоянии одного вируса. 7-9 классы. Внеурочная деятельность. – М.: Просвещение, 2019 – 80 с.
10. Основы кибербезопасности.
<https://www.xn--d1abkefqip0a2f.xnp1ai/index.php/glava-1-osnovy-kiberbezopasnosti-tseli-i-zadachi-kurs>
11. Цифровая компетентность подростков и родителей. Результаты всероссийского исследования / Г.У. Солдатова, Т.А. Нестик, Е.И. Рассказова, Е.Ю. Зотова. – М.: Фонд Развития Интернет, 2013 – 144 с.