

МИНИСТЕРСТВО ПРОСВЕЩЕНИЯ РОССИЙСКОЙ ФЕДЕРАЦИИ
Департамент образования Ивановской области
Управление образования Кинешемского муниципального района
МОУ Решемская средняя школа

<p>РАССМОТРЕНО на заседании педагогического совета</p> <hr/> <p>Потапенко Л.В. протокол №5 от «29» августа 2023 г.</p>	<p>УТВЕРЖДЕНО приказом директора МОУ Решемской средней школы</p> <hr/> <p>Власова В.Р. Приказ № 72 от «29» августа 2023 г.</p>
--	--

РАБОЧАЯ ПРОГРАММА
УЧЕБНОГО КУРСА
«ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ»
ДЛЯ ОБРАЗОВАТЕЛЬНЫХ ОРГАНИЗАЦИЙ, РЕАЛИЗУЮЩИХ
ПРОГРАММЫ ОСНОВНОГО ОБЩЕГО ОБРАЗОВАНИЯ

Составитель:
Балашова О.В. –
учитель высшей кв. категории

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 их возрастных особенностей. Программа курса ориентирована на включение в контекст обучения и воспитания новых видов информационных угроз и средств противодействия им. Программа курса разработана для 7—9 классов.

Реализация программы учебного курса возможна в разных формах:

- как дополнительные модули обучения в интеграции с предметами «Информатика» и (или) «ОБЖ» для 7—9 классов (от 30 учебных часов 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.

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

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.

СОДЕРЖАНИЕ УЧЕБНОГО КУРСА «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.

7—9 классы

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 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.

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.

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.

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.

ТЕМАТИЧЕСКОЕ ПЛАНИРОВАНИЕ КУРСА «ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ»

7—9 классы

Программа учебного курса для 7—9 классов основного общего образования рассчитана на объем не менее 30 часов. Программа курса может быть реализована по выбору образовательной организации как самостоятельный учебный курс во внеурочной деятельности детей за один год обучения или отдельными модулями в программах освоения учебных предметов «Информатика» и (или) «ОБЖ» (в 7—9 классах), а также в рамках школьных мероприятий с участием родителей интегрирована модулями в календарное планирование программы воспитания.

Варианты учебного планирования:

Вариант 1. Планирование обучения за один год обучения. Один урок в неделю. 30 уроков.

Вариант 2. Планирование обучения по модулям в 7—9 классах. Модуль 1, всего 10 уроков.

Модуль 2, всего 10 уроков.

Модуль 3, всего 10 уроков.

Модуль/тема	Всего часов	Теоретические занятия	Практическая работа ресурсами и программами на компьютере
<i>Линия «Информационное общество и информационная культура»</i>	20	9	11

Модуль 1. Современное информационное пространство и искусственный интеллект	10	5	5
1.1. Киберпространство. Кибермиры. Киберфизическая система	5	2	3
1.2. Киберобщество. Киберденьги. Кибермошенничество	5	3	2
Модуль 2. Современная информационная культура	10	4	6
2.1. Киберкультура. От книги к гипертексту. Киберкнига. Киберискусство.	4	2	2
2.2. Социальная инженерия. Классификация угроз социальной инженерии	4	2	2
2.3. Новые профессии в киберобществе. Цифровизация профессий	2		2
<i>Линия «Информационное пространство и правила информационной безопасности»</i>	10	4	6
Модуль 3. Угрозы информационной безопасности	10	4	6
3.1. Киберугрозы. Кибервойны. Киберпреступность. Уязвимости кибербезопасности. Угрозы информационной безопасности. Запрещенные и нежелательные сайты	4	2	2
3.2. Защита от вредоносных программ и информационных атак	3	1	2
3.3. Практика электронного обучения в сфере информационной безопасности	3	1	2
Всего:	30	13	17