

**Министерство образования, науки и молодежной политики
Краснодарского края**

**Государственное бюджетное образовательное учреждение
дополнительного профессионального образования «Институт развития
образования» Краснодарского края**

**Дополнительная профессиональная программа
(повышение квалификации)**

**Формирование медиаграмотности и информационной культуры
обучающихся в условиях образовательной организации**

Разработчик(и) программы:

**Чиркова Т.Н., Государственное бюджетное образовательное учреждение
дополнительного профессионального образования «Институт развития
образования» Краснодарского края, нет**

Раздел 1. Характеристика программы

1.1. Цель реализации программы - совершенствование профессиональных компетенций слушателей в области формирования медиаграмотности и информационной культуры обучающихся в условиях образовательной организации.

1.2. Планируемые результаты обучения:

Учитель

Трудовая функция	Трудовое действие	Знать	Уметь
Развивающая деятельность (приказ Минтруда России от 18.10.2013 № 544н «Об утверждении профессионального стандарта «Педагог (педагогическая деятельность в сфере дошкольного, начального общего, основного общего, среднего общего образования) (воспитатель, учитель)» (зарегистрирован в Минюсте России 06.12.2013 № 30550)	Формирование и реализация программ развития универсальных учебных действий, образцов и ценностей социального поведения, навыков поведения в мире виртуальной реальности и социальных сетях, формирование толерантности и позитивных образцов поликультурного общения	Приоритетные направления развития образовательной системы Российской Федерации, действующие нормативные документы в области информационной безопасности детей. Основные информационные угрозы и механизмы защиты детей от информационных угроз. Основные направления профилактической работы по обеспечения информационной безопасности обучающихся в образовательной организации.	Проектировать меры по обеспечению информационной безопасности обучающихся в образовательной организации. Применять технологию девиантологического анализа медиапродукции. Планировать профилактическую работу по формированию у обучающихся сознательного и ответственного поведения в информационном пространстве.

Социальный педагог

Трудовая функция	Трудовое действие	Знать	Уметь
Планирование мер по социально-педагогической поддержке обучающихся в процессе социализации (приказ Минтруда России от 10.01.2017 № 10н "Об утверждении профессионального стандарта «Специалист в области воспитания» (зарегистрирован в Минюсте России 26.01.2017 № 45406)	Разработка мер по профилактике социальных девиаций среди обучающихся	Приоритетные направления развития образовательной системы Российской Федерации, действующие нормативные документы в области информационной безопасности детей. Основные информационные угрозы и механизмы защиты детей от информационных угроз. Основные направления профилактической работы по обеспечения информационной безопасности обучающихся в образовательной организации.	Проектировать меры по обеспечению информационной безопасности обучающихся в образовательной организации. Применять технологию девиантологического анализа медиапродукции. Планировать профилактическую работу по формированию у обучающихся сознательного и ответственного поведения в информационном пространстве.

Педагог-психолог

Трудовая функция	Трудовое действие	Знать	Уметь

<p>Психологическая профилактика (профессиональная деятельность, направленная на сохранение и укрепление психологического здоровья обучающихся в процессе обучения и воспитания в образовательных организациях) (приказ Минтруда России от 24.07.2015 № 514н «Об утверждении профессионального стандарта «Педагог-психолог (психолог в сфере образования)» (зарегистрирован в Минюсте России 18.08.2015 № 38575)</p>	<p>Планирование и реализация совместно с педагогом превентивных мероприятий по профилактике возникновения социальной дезадаптации, аддикций и девиаций поведения</p>	<p>Приоритетные направления развития образовательной системы Российской Федерации, действующие нормативные документы в области информационной безопасности детей. Основные информационные угрозы и механизмы защиты детей от информационных угроз. Основные направления профилактической работы по обеспечения информационной безопасности обучающихся в образовательной организации.</p>	<p>Проектировать меры по обеспечению информационной безопасности обучающихся в образовательной организации. Применять технологию девиантологического анализа медиа-продукции. Планировать профилактическую работу по формированию у обучающихся сознательного и ответственного поведения в информационном пространстве.</p>
---	--	---	---

1.3. Категория слушателей:

педагогические работники (учителя, педагоги-психологи, социальные педагоги)

1.4. Форма обучения - Очная

1.5. Срок освоения программы: 36 ч.

Раздел 2. Содержание программы

№ п/п	Наименование разделов (модулей) и тем	Всего часов	Виды учебных занятий, учебных работ		Самостоятельная работа, час	Формы контроля
			Лекция, час	Интерактивное (практическое) занятие, час		
	Входная диагностика	1	0	0	1	
1	Государственная политика в сфере общего образования Российской Федерации. Законодательство Российской Федерации о защите детей от информации, причиняющей вред их здоровью и (или) развитию	7	5	2	0	практическая работа
	Промежуточная аттестация по 1 модулю	1	0	0	1	тест
2	Современные информационные угрозы и обеспечение информационной безопасности обучающихся	0	0	0	0	
2.1	Виды информационных угроз.	6	4	2	0	практическая работа

2.2	Обеспечение информационной безопасности обучающихся в условиях образовательной организации	6	4	2	0	кейс
	Промежуточная аттестация по 2 модулю	1	0	0	1	тест
3	Развитие медиаграмотности и информационной культуры обучающихся	0	0	0	0	
3.1	Медиаграмотность и информационная культура, способы формирования.	6	6	0	0	
3.2	Технология девиантологического анализа медиапродукции	4	0	4	0	практическая работа
	Итоговая аттестация	4	0	4	0	проект
	Итого	36	19	14	3	

2.2. Рабочая программа

1 Государственная политика в сфере общего образования Российской Федерации.

Законодательство Российской Федерации о защите детей от информации, причиняющей вред их здоровью и (или) развитию (лекция - 5 ч. практическое занятие - 2 ч.)

Лекция·Государственная политика в сфере общего образования Российской Федерации. Цели и ключевые задачи Российской Федерации в сфере образования. Суть цифровой трансформации образования. Нормативное регулирование информационной безопасности обучающихся. Федеральный закон «О защите детей от информации, причиняющей вред их здоровью и развитию» от 29.10.2012 года № 436-ФЗ. Приказ Министерства цифрового развития, связи и массовых коммуникаций РФ от 01.12.2020 г. № 644 «О плане мероприятий, направленных на обеспечение информационной безопасности детей, на 2021 – 2027 годы». Способы обеспечения информационной безопасности обучающихся в образовательной организации. Локальные акты образовательной организации, направленные на обеспечение медиабезопасности обучающихся.

Практическая работа·Подготовка отчета по основным нормативно-правовым актам Российской Федерации о защите детей от информации, причиняющей вред их здоровью и (или) развитию. Цель: анализ и систематизация нормативно –правовых документов в сфере защиты детей от информации, причиняющей вред их здоровью и (или) развитию. Результат: систематизация нормативно-правовой документации в сфере защиты детей от информации, причиняющей вред их здоровью и (или) развитию.

2 Современные информационные угрозы и обеспечение информационной безопасности обучающихся

2.1 Виды информационных угроз. (лекция - 4 ч. практическое занятие - 2 ч.)

Лекция·Воздействие информационной среды на социализацию современных детей и молодёжи (формирование зависимости, виртуализация сознания, «клиповое мышление»). Понятие «угроза информационной безопасности» и классификация угроз Понятие «угроза информационной безопасности». Классификация угроз. Технические угрозы (возможность повреждения ПО, информации, нарушение ее конфиденциальности или взлома аккаунта, хищения паролей и персональной информации). Коммуникационные угрозы (кибербуллинг, рекрутинг в опасные и экстремистские сообщества и др.). Контентные угрозы (закрытые группы смерти, группы «вписки» и др.). Потребительские угрозы (риск приобретения товара

низкого качества, подделок, контрафактной и фальсифицированной продукции, хищение денежных средств злоумышленником через онлайн-банкинг и т.д.)

Практическая работа·Анализа аккаунтов в социальных сетях с целью выявления распространения информации, склоняющей к деструктивному поведению. Цель: совершенствование навыков выявления прямых и косвенных признаков деструктивного поведения на основании медиаконтента представленного на странице в социальной сети. Результат: формирование умения анализировать медиаконтент на предмет наличия информации склоняющей несовершеннолетних к деструктивному поведению.

2.2 Обеспечение информационной безопасности обучающихся в условиях образовательной организации (лекция - 4 ч. практическое занятие - 2 ч.)

Лекция·Способы обеспечения информационной безопасности обучающихся в образовательной организации. Локальные акты образовательной организации, направленные на обеспечение медиабезопасности обучающихся. Методы защиты от вредоносного ПО. Требования к информационной безопасности при работе в общедоступных сетях Wi-fi. Санитарно - гигиенические требования к организации занятий с использованием цифровых средств обучения. Алгоритм работы образовательной организации по мониторингу аккаунтов обучающихся в социальных сетях с целью выявления информации, склоняющей к деструктивному и противоправному поведению

Практическая работа·Обеспечение информационной безопасности обучающихся в условиях образовательной организации. Решение кейсов. Цель: отработка навыков анализа проблемной ситуации и определение стратегии по обеспечению информационной безопасности обучающихся в образовательной организации, на основании представленной информации. Результат: формирование умения оценивать информационные риски ситуации и выработка стратегии по обеспечению информационной безопасности обучающихся в условиях образовательной организации.

3 Развитие медиаграмотности и информационной культуры обучающихся

3.1 Медиаграмотность и информационная культура, способы формирования. (лекция - 6 ч.)

Лекция·Информационная культура личности как часть общей культуры современного человека. Формирование у обучающихся навыков безопасного использования цифровых технологий. ·Понятие «персональные данные». Виды персональных данных. «Цифровые следы» и идентификация пользователей сетей. ·Средства защиты персональных данных. Приватность и личные границы в сети Интернет. Правила безопасных коммуникаций в сети Интернет. Алгоритм действий при столкновении с ситуациями кибербуллинга, вовлечения в деструктивные Интернет-сообщества.

3.2 Технология девиантологического анализа медиапродукции (практическое занятие - 4 ч.)

Практическая работа·Проведение девиантологического анализа медиапродукции кинофильма/мультифильма/музыкального видеоклипа. Цель: совершенствование навыков анализа медиаконтента на предмет наличия деструктивных посылов для организации профилактической работы с обучающимися Результат: отработка практических навыков применения методики девиантологического анализа медиапродукции, оценка медиаконтента на предмет деструктивных посылов.

Раздел 3. Формы аттестации и оценочные материалы

Входной контроль

Форма: тестирование

Описание, требования к выполнению:

Описание, требования к выполнению: Тест включает 10 вопросов с выбором ответа. Вопросы охватывают основные проблемы подлежащие изучению в процессе обучения. Каждый верный

ответ оценивается в 1 балл.

Критерии оценивания:

Каждый правильный ответ оценивается в 1 балл. Входное тестирование считается пройденным, если слушатель ответил на 6 вопросов и более.

Примеры заданий:

1. Является ли верным утверждение: контентные угрозы — это материалы, содержащие насилие, агрессию, эротику и порнографию, нецензурную лексику, информацию, разжигающую расовую ненависть, пропаганду анорексии и булимии, суицида, азартных игр, наркотических веществ и т.д.

Выберите один ответ:

а) да

б) нет

2. Способы помочи ребенку (подростку), ставшему жертвой кибербуллинга (выберите все верные варианты ответа):

а) запрет на использование сети Интернет;

б) обсуждение с ребенком правил кибербезопасности;

в) сохранение свидетельств кибербуллинга (сообщений с угрозами и нежелательным контентом);

г) снижение значимости травли в киберпространстве (объяснить ребенку, что на это можно не обращать внимание);

д) обучение дифференцированной реакции на киберагgression: игнорирование единичных фактов агрессии, блокировка агрессивных пользователей, но при повторяющихся фактах агрессии – обращение за помощью к взрослым.

Количество попыток: не ограничено

Текущий контроль

Раздел программы: 1. Государственная политика в сфере общего образования Российской Федерации. Законодательство Российской Федерации о защите детей от информации, причиняющей вред их здоровью и (или) развитию

Форма: практическая работа

Описание, требования к выполнению:

Составление отчета. Отчет представляет собой оформленный и кратко аннотированный перечень нормативно-правовых актов в сфере информационной безопасности несовершеннолетних, сгруппированный в иерархическом порядке.

Критерии оценивания:

полнота охвата действующих нормативно-правовых актов, иерархия нормативно-правовых актов, качество аннотирования. Оценка «зачтено» выставляется слушателю, выполнившему практическое задание в полном объеме, корректно составившему иерархию. Оценка «не зачтено» выставляется, если слушатель выполнил неверно практическое задание.

Примеры заданий:

Составьте краткий аннотированный перечень нормативно-правовых актов в сфере информационной безопасности несовершеннолетних . Список должен быть составлен в иерархическом порядке.

Количество попыток: не ограничено

Раздел программы: 2.1 Виды информационных угроз.

Форма: Практическая работа

Описание, требования к выполнению:

Проведение мониторинга предложенных аккаунтов на предмет наличия информации содержащей деструктивные посылы. Практическая работа должна быть выполнена на листах формата А4, шрифт – Times New Roman; кегль (размер шрифта) – 14 пт; межстрочный интервал – 1,5. Объем не ограничен.

Критерии оценивания:

Оценка «зачтено» выставляется слушателю, выполнившему практическое задание в полном объеме, корректно сделавшему выводы на основе представленной информации. Оценка «не зачтено» выставляется, если слушатель выполнил неверно практическое задание.

Примеры заданий:

Проведите анализ предоставленных аккаунтов в сети ВКонтакте на предмет наличия информации содержащей деструктивные посылы.

После анализа аккаунтов, слушателям предлагается ответить на вопросы.

Примеры вопросов:

1. Содержать ли данные страницы в социальных сетях девиантологическую информацию?
2. Нарушает ли представленная в аккаунте информация законы Российской Федерации?
3. Является ли контент, представленный на предложенной странице экстремистским?

Количество попыток: не ограничено

Раздел программы: 2.2.Обеспечение информационной безопасности обучающихся в условиях образовательной организации

Форма: практическая работа (решение кейса)

Описание, требования к выполнению:

Слушателям предлагается провести анализ предложенного кейса по заданным параметрам: 1) участники ситуации 2) нарушение законодательства Российской Федерации 3) нормативно-правовое обоснование деятельности педагогических работников и разработать проект плана мер по обеспечению информационной безопасности обучающихся в конкретной ситуации.

Критерии оценивания:

Оценка «зачтено» выставляется слушателю, выполнившему практическое задание в полном объеме, предложен корректный план мер. Оценка «не зачтено» выставляется, если слушатель выполнил неверно практическое задание.

Примеры заданий:

Кейс № 1. Ученица 7 класса рассказала своему классному руководителю, что ее одноклассники снимает на фото и видео все, что происходит на переменах. Чтобы контент был интересным, они берут чужие вещи и выбрасывают их в мусорку, и ждут, когда владелец вещи начнет ее искать. Фото и видео ученики выкладывают в разные социальные сети.

Кейс № 2. Заместитель директора по учебно-воспитательной работе получает обращение от родителя ученика. В тексте обращения говорится о том, что в социальных сетях распространяется снимок, на котором виден список учеников класса и их оценки. К жалобе прилагаются скриншоты страницы социальной сети. Родитель просит принять меры. Заместитель директора понимает, что фото с оценками обучающихся сделано с экрана компьютера учителя.

Кейс № 3. К психологу школы за советом обратился ученик 6 класса. Ученик рассказал, что около недели назад по электронной почте он получил приглашение от своего друга поиграть в Интернет-игру. Перейдя по ссылке, он окне подтвердил свое участие, нажав какую-то кнопку. Игра оказалась очень увлекательной, но спустя день на электронную почту пришло письмо с незнакомого адреса с требованием оплаты участия. Ученик его проигнорировал, однако письма стали появляться каждый день и содержать угрозы благополучию его семьи. Со слов ученика он должен уже около 5000 рублей. Родителям рассказать боится. Что предпринять не знает.

Количество попыток: не ограничено

Раздел программы: 3.2. Технология девиантологического анализа медиапродукции

Форма: практическая работа

Описание, требования к выполнению:

Выполните девиантологический анализ медиапродукции предложенного медиапродукта.

Заполните таблицу предоставленную в методике.

Критерии оценивания:

Оценка «зачтено» выставляется слушателю, грамотно выполнившему анализ предложенного медиапродукта, возможно допущение незначительных ошибок, не имеющие принципиального характера. Практическая работа требует доработки в случаях, если слушатель выполнил неверно практическое задание.

Примеры заданий:

Выполните девиантологический анализ медиапродукции (кинофильма/мультифильма/музыкального видеоклипа) с помощью методики С.В. Книжниковой с целью определения характера его возможного влияния на детскую (подростковую, молодежную) аудиторию.

1. Серия мультфильма «Смешарики»
2. Художественный фильм «Приключения электроника»
3. Современный музыкальный клип

Количество попыток: не ограничено

Промежуточный контроль

Раздел программы: 1. Государственная политика в сфере общего образования Российской Федерации. Законодательство Российской Федерации о защите детей от информации, причиняющей вред их здоровью и (или) развитию

Форма: Тест

Описание, требования к выполнению:

10 заданий с выбором одного или нескольких правильных ответов. Время на выполнение – 45 минут.

Критерии оценивания:

Каждый правильный ответ оценивается в 1 балл. В заданиях с выбором нескольких правильных ответов 1 балл зачитывается только при выборе всех правильных ответов.

Тестирование считается пройденным, если слушатель набрал более 7 баллов – «зачтено», если

менее 7 баллов – «не зачтено».

Примеры заданий:

1. Согласно Федеральному закону от 29 декабря 2010 г. N 436-ФЗ "О защите детей от информации, причиняющей вред их здоровью и развитию" к информации, причиняющей вред здоровью и (или) развитию детей, относится (выберите несколько правильных ответов):

А) побуждающая детей к совершению действий, представляющих угрозу их жизни и (или) здоровью, в том числе к причинению вреда своему здоровью, самоубийству, либо жизни и (или) здоровью иных лиц, либо направленная на склонение или иное вовлечение детей в совершение таких действий;

Б) способная вызвать у детей желание употребить наркотические средства, психотропные и (или) одурманивающие вещества, табачные изделия, никотинсодержащую продукцию, алкогольную и спиртосодержащую продукцию, принять участие в азартных играх, заниматься проституцией, бродяжничеством или попрошайничеством;

В) обосновывающая или оправдывающая допустимость насилия и (или) жестокости либо побуждающая осуществлять насильственные действия по отношению к людям или животным;

Г) содержащая изображение или описание эротического характера;

Д) отрицающая семейные ценности, пропагандирующая нетрадиционные сексуальные отношения и формирующая неуважение к родителям и (или) другим членам семьи;

Е) содержащая нецензурную брань.

2. Какие приоритетные задачи устанавливает Концепция информационной безопасности детей для семьи, государства и организаций, заинтересованных в обеспечении информационной безопасности детей?

А) повышение уровня медиаграмотности детей

Б) усвоение детьми системы семейных ценностей

В) формирование у детей навыков по выбору правильного образовательного профиля

Г) сохранение конфиденциальности документированной информации

3. Информационная безопасность детей представляет собой:

А) совокупность материальных и духовных ценностей в области информации;

Б) состояние защищенности детей, при котором отсутствует риск, связанный с причинением информацией, в том числе распространяемой в сети Интернет, вреда их здоровью, физическому, психическому, духовному и нравственному развитию;

В) грамотное использование детьми и их педагогами инструментов, обеспечивающих доступ к информации, развитие критического анализа содержания информации и привития коммуникативных навыков.

Количество попыток: не ограничено

Раздел программы: 2. Современные информационные угрозы и обеспечение информационной безопасности обучающихся

Форма: тест

Описание, требования к выполнению:

10 заданий с выбором одного или нескольких правильных ответов. Время на выполнение – 45

минут.

Критерии оценивания:

Каждый правильный ответ оценивается в 1 балл. В заданиях с выбором нескольких правильных ответов 1 балл зачитывается только при выборе всех правильных ответов. Тестирование считается пройденным, если слушатель набрал более 7 баллов – «зачтено», если менее 7 баллов – «не зачтено».

Примеры заданий:

1. К коммуникационным рискам в сети Интернет относятся (выберите один правильный ответ):

- А) вредоносные программы (вирусы, черви, трояны), повреждающие программное обеспечение;
- Б) взломы аккаунта, хищение паролей и персональной информации;
- В) кибербуллинг, рекрутинг в опасные и экстремистские сообщества;
- Г) знакомства с целью сексуального использования;
- Д) пропаганда девиантного поведения.

2. К основным признакам Интернет-зависимости не относится:

- А) создание и эксплуатация виртуальных образов, крайне далеких от реальных;
- Б) субъективно воспринимаемая невозможность обходиться без работы в сети;
- В) общение в чатах, участие в телеконференциях.

3. Под информационной безопасностью понимается:

- А) защищенность информации и поддерживающей инфраструктуры от случайных или преднамеренных действий естественного или случайного характера, которые могут нанести неприемлемый ущерб субъектам информационных отношений в том числе владельцам и пользователям информации и поддерживающей инфраструктуре
- Б) программный продукт и базы данных должны быть защищены по нескольким направлениям от воздействия
- В) комплекс мер по предотвращению вероятности несанкционированного доступа к системе
- Г) нет правильного ответа

Количество попыток: не ограничено

Итоговая аттестация

Форма: Разработка проекта

Описание, требования к выполнению:

Разработать проект занятия по развитию медиаграмотности и культуры обучающихся в области использования ИКТ. Возрастная категория обучающихся на выбор: младший школьный возраст, подростковый возраст, юношеский возраст. Защита итогового проекта проходит в виде презентации своего проекта с дальнейшим обсуждением. Цель: оценка уровня профессиональных компетенций слушателей в области формирования медиаграмотности и информационной культуры обучающихся в условиях образовательной организации.

Критерии оценивания:

- 1. Актуальность предложенной темы.
- 2. Наличие структурных элементов, определение целей и задач.
- 3. Содержательное наполнение занятия.
- 4. Использование различных форм/видов

учебной деятельности 5. Наличие инструментов контроля достижения поставленной цели занятия (формирования у обучающихся медиаграмотности и информационной культуры). Показатели оценивания по каждому критерию: - высокий уровень: полностью соответствует заявленным критериям – 2 балла; - средний уровень: частично соответствует заявленным критериям – 1 балл; низкий уровень: не соответствует заявленным критериям – 0 баллов. Максимальная оценка- 10 баллов. Итоговая аттестация оценивается по системе «зачтено» / «не зачтено». Оценка «зачтено» – 6 и более баллов. Оценка «не зачтено» - менее 6 баллов.

Примеры заданий:

Пример: Разработать проект занятия направленного на профилактику зависимости от социальных сетей и мессенджеров для обучающихся 5-7 классов.

Количество попыток: не ограничено

Раздел 4. Организационно-педагогические условия реализации программы

4.1. Организационно-методическое и информационное обеспечение программы

Нормативные документы

1. Об образовании в Российской Федерации [Электронный ресурс]: федер. закон от 29.12.2012 № 273-ФЗ. Доступ из справ.-правовой системы «КонсультантПлюс» URL: http://www.consultant.ru/document/cons_doc_LAW_140174/
2. О внесении изменений в Федеральный закон «Об образовании в Российской Федерации» по вопросам воспитания обучающихся [Электронный ресурс]: федер. закон от 31.07.2020 № 304-ФЗ. Доступ из справ.-правовой системы «Гарант». URL: <https://www.garant.ru/products/ipo/prime/doc/74351950/>
3. О персональных данных [Электронный ресурс]: федер. закон от 27.07.2006 N 152-ФЗ (последняя редакция). Доступ из справ.-правовой системы «КонсультантПлюс». URL: http://www.consultant.ru/document/cons_doc_LAW_61801/
4. О защите детей от информации, причиняющей вред их здоровью и развитию [Электронный ресурс]: федер. закон от 29.12.2010 г. № 436-ФЗ (с изменениями от 01.05.2019). Доступ из справ.-правовой системы «Гарант». URL : <https://base.garant.ru/12181695/>
5. О Стратегии развития информационного общества в Российской Федерации на 2017 - 2030 годы [Электронный ресурс]: указ Президента РФ от 9.05.2017 № 203. Доступ из справ.-правовой системы «Гарант». URL : <https://www.garant.ru/products/ipo/prime/doc/71570570/>
6. Концепция информационной безопасности детей [Электронный ресурс]: распоряжение Правительства РФ от 02.12.2015 № 2471-р // Официальный интернет-портал правительства России. URL:<http://static.government.ru/media/files/mPbAMyJ29uSPhL3p20168GA6hv3CtBxD.pdf>
7. План основных мероприятий, проводимых в рамках Десятилетия детства, на период до 2027 года [Электронный ресурс]: распоряжение Правительства РФ от 23.01.2021 №122-р. Доступ из справ.-правовой системы «Гарант». URL : <https://www.garant.ru/products/ipo/prime/doc/400150053/>
8. Об утверждении профессионального стандарта «Специалист в области воспитания» [Электронный ресурс]: Приказ Министерства труда и социальной защиты РФ от 10 января 2017 года № 10н. Доступ из справ.-правовой системы «Гарант». URL: <https://www.garant.ru/products/ipo/prime/doc/71495630/>

9. Об утверждении профессионального стандарта «Педагог - психолог»: Приказ Министерства труда и социальной защиты РФ от 24.07.2015 № 514н. URL: <https://base.garant.ru/71166760/>
10. Профессиональный стандарт «Педагог (педагогическая деятельность в дошкольном, начальном общем, основном общем, среднем общем образовании) (воспитатель, учитель)» [Электронный ресурс]: приказ Министерства труда и социальной защиты РФ от 18.10.2013 № 544н. Доступ из справ.-правовой системы «Гарант». URL: <https://base.garant.ru/70535556/>
11. О плане мероприятий, направленных на обеспечение информационной безопасности детей, на 2021 - 2027 годы [Электронный ресурс]: приказ Министерства цифрового развития, связи и массовых коммуникаций РФ от 01.12.2020 № 644. Доступ из справ. правовой системы «Гарант». URL : <https://base.garant.ru/75011297>

Литература

1. Алгоритм действий для родителей обучающихся по раннему выявлению и реагированию на деструктивное поведение несовершеннолетних, проявляющееся под воздействием информации негативного характера, распространяемой в сети Интернет. АНО «Центр изучения и сетевого мониторинга молодежной среды»; ФГБУ «Центр защиты прав и интересов детей». М., 2020. 24 с.
2. Гендина Н.И., Косолапова Е.В., Рябцева Л.Н. Информационная культура личности в 2 ч. Часть 1: учебное пособие для вузов / под науч. ред. Н.И. Гендиной. Изд 2-е, М.: Издательство Юрайт, 2021. 356 с.
3. Книжникова С.В. Подготовка подростков к осознанному выявлению в медиапродукции девиантных установок: монография. Краснодар: Экоинвест, 2014. 149 с.
4. Медийно-информационная грамотность в цифровом мире: как научить учителей: сборник статей / под ред. Ю.Ю. Черного, Т.А. Мурованы. М.: Институт ЮНЕСКО по информационным технологиям в образовании, 2021. 81 с.
5. Нестеров С.А. Информационная безопасность: учебник и практикум . Санкт-Петербург : Лань, 2021. 324с.
6. Основы цифровой грамотности и кибербезопасности: учеб. пособие / Т.А. Бороненко [и др.]. СПб.: ЛГУ им. А.С. Пушкина, 2021. 431 с.

Электронные обучающие материалы

Интернет-ресурсы

1. Медийно-информационная грамотность. Институт ЮНЕСКО по информационным технологиям в образовании: [сайт]. URL: <https://iite.unesco.org/ru/mig/>
2. Информационно-правовой портал КонсультантПлюс: [сайт]. URL:<http://www.consultant.ru/>
3. Сайт Единого урока по безопасности в сети «Интернет»: [сайт]. URL: www.Единыйурок.рф
4. Всероссийский проект «Медиаграмотность» Российское движение школьников: [сайт]. URL: <https://xn--d1axz.xn--p1ai/competition/107>

4.2. Материально-технические условия реализации программы

Технические средства обучения

Подключение к сети Интернет - (широкополосный) проводной или беспроводной (3G или 4G/LTE). Динамики и микрофон - встроенные или USB, или беспроводные Bluetooth Веб-камера или HD-веб-камера - встроенная или USB или HDвидеокамера.

Персональный компьютер, ноутбук, ультрабук, нетбук; планшетный компьютер; смартфон
Операционные системы: Windows7 и выше, MacO8 X, 10.7 и выше.