

МИНИСТЕРСТВО ОБРАЗОВАНИЯ И НАУКИ КАРАЧАЕВО-ЧЕРКЕССКОЙ РЕСПУБЛИКИ  
РГБУ ДПО «КАРАЧАЕВО-ЧЕРКЕССКИЙ РЕСПУБЛИКАНСКИЙ ИНСТИТУТ  
ПОВЫШЕНИЯ КВАЛИФИКАЦИИ РАБОТНИКОВ ОБРАЗОВАНИЯ»

**Центр непрерывного повышения педагогического мастерства**

Решение Ученого  
совета  
РГБУ ДПО  
«КЧРИПКРО»  
от «13» 03  
2022 г.  
Протокол № 50

**УТВЕРЖДАЮ**  
Ректор РГБУ ДПО «КЧРИПКРО»  
А.В. Гурин  
«  »    2022 г.



**Дополнительная профессиональная программа  
(повышение квалификации)**

**Информационная безопасность детей: социальные и технологические  
аспекты**

**Разработчик(и) программы:  
Важинская И.А.  
Черкасова Э.В.**

**Категория слушателей:** учителя общеобразовательных организаций, преподаватели  
СПО, специалисты системы ДОО.  
**Количество часов:** 18 ч

Черкесск, 2022

## Раздел 1. Характеристика программы.

1.1. **Цель реализации программы:** совершенствование профессиональных компетенций слушателей в области формирования информационной безопасности детей: социальных и технологических аспектов.

1.2. **Планируемые результаты обучения.**

<b>Трудовые действия (Профстандарт «Педагог» Общепедагогическая функция. Обучение.)</b>	<b>Знать</b>	<b>Уметь</b>
1. Планирование и проведение учебных занятий 2. Формирование навыков, связанных с информационно-коммуникационными технологиями. 3. Регулирование поведения обучающихся для обеспечения безопасной образовательной среды	- приоритетные направления развития образовательной системы Российской Федерации; - действующие нормативные документы в области информационной безопасности детей; - основные информационные угрозы; - основные механизмы защиты детей от информационных угроз.	- применять механизмы выявления и защиты детей от основных социальных угроз; - применять механизмы выявления и защиты детей от возникающих угроз при работе с персональными устройствами;

1.3 **Категория обучающихся** учителя общеобразовательных организаций, преподаватели СПО, специалисты системы ДОО

1.4 **Форма обучения:** заочная с применением дистанционных образовательных технологий (онлайн-курс).

1.5. **Срок освоения программы:** 18 часов.

## Раздел 2. Содержание программы.

### 2.1. Учебный (тематический) план.

№ п/п	Наименование разделов, модулей, тем	Всего часов	Виды учебных занятий				Форма контроля	
			Аудиторные занятия		Дистанционные образовательные технологии			
			Лекции	Практические	Лекции	Практические		
<b>1.</b>	<b>Модуль 1. Приоритетные направления государственной образовательной политики</b>	<b>6</b>			<b>4</b>	<b>2</b>		
<b>1.1</b>	Входное тестирование	<b>1</b>				1	Тест	Текущий контроль
<b>1.2</b>	Государственная политика в сфере общего образования РФ	<b>2</b>			<b>2</b>			
<b>1.3</b>	Нормативное регулирование в области информационной безопасности детей.	<b>2</b>			<b>2</b>			
<b>1.4</b>	Цифровая трансформация образования.	<b>2</b>				<b>2</b>	Тест	Текущий контроль
<b>2.</b>	<b>Модуль 2. Планирование и организация деятельности по защите детей от угроз сети Интернет</b>	<b>10</b>			<b>2</b>	<b>8</b>		
<b>2.1</b>	Планирование и организация деятельности по обеспечению информационной безопасности в	<b>2</b>				<b>2</b>		

	образовательной организации							
2.2	Планирование и организация деятельности по выявлению угроз в сети Интернет	2				2		
2.3	Планирование и организация деятельности по защите от вредоносных программ	2				2		
2.4	Планирование и организация деятельности по Безопасному использованию интеллектуальной собственности и предотвращению нарушений авторского права	2			2			
2.5	Планирование и организация деятельности по внедрению в практику образовательной организации правил сетевой гигиены	2				2	Тест	Промежуточная аттестация
<b>3</b>	<b>Модуль 3. Итоговая аттестация</b>							
	Выходное тестирование.	<b>1</b>				<b>1</b>	Зачет	
	<b>Итого:</b>	<b>18</b>			<b>6</b>	<b>12</b>		

### 2.1.1. Учебный план

дополнительной профессиональной программы повышения квалификации «Информационная безопасность детей: социальные и технологические аспекты»

**Цель:** совершенствование профессиональных компетенций слушателей в области формирования информационной безопасности детей: социальных и технологических аспектов.

**Категория слушателей:** учителя общеобразовательных организаций, преподаватели СПО, специалисты системы ДОО

**Количество часов:** 18 часов.

**Режим занятий:** 6-8 часов в день.

**Форма обучения:** очно-дистанционная.

№ п/п	Наименование разделов, модулей, тем	Всего часов	Аудиторные учебные занятия, учебные работы		Внеаудиторная работа, час	Формы контроля (и формы проведения)	Трудоемкость, час
			Лекции	Практические			
<b>Базовая часть</b>							
<b>Р1</b>		<b>Основы законодательства Российской Федерации в области образования</b>					
	<b>Модуль 1. Приоритетные направления государственной образовательной политики</b>	<b>6</b>	<b>4</b>	<b>2</b>			<b>6</b>
	Входное тестирование	<b>1</b>		<b>1</b>		Тест	
<b>Профильная часть</b>							
<b>Р2</b>		<b>Предметно-методическая деятельность</b>					
	<b>Модуль 2. Планирование организация деятельности по защите детей от угроз сети Интернет</b>	<b>10</b>	<b>2</b>	<b>8</b>		Текущий контроль	<b>10</b>
<b>Итоговая аттестация</b>							
	<b>Модуль 3. Итоговая аттестация</b>	<b>1</b>		<b>1</b>			
	Выходное тестирование. Зачет	<b>1</b>		<b>1</b>			Тест
	<b>Итого:</b>	<b>18</b>	<b>6</b>	<b>12</b>			

## 2.1. Календарный учебный график

дополнительной профессиональной программы повышения квалификации

Наименование	Виды учебной нагрузки	Порядковые номера недель обучения	всего
		1	
«Информационная безопасность детей: социальные и технологические аспекты»	Лекции, практические занятия	Л-0 П-0	Л-0 П-0
	(дистанционная) работа	Л-6 П-12	Л-6 П-12
	Итоговая аттестация: Зачет	1	1

В календарный учебный график могут вноситься изменения при составлении расписания занятий для каждой группы слушателей

## 2.2. Содержание учебной программы

№ п/п	Наименование тем	Виды учебных занятий, учебных работ	Содержание
<b>1.</b>	<b>Модуль 1. Приоритетные направления государственной образовательной политики.</b>		
<b>1.1</b>	Входное тестирование	Практическое занятие  1 ч.	Проводится для того чтобы определить степень владения необходимыми (базовыми) знаниями и умениями для изучения предлагаемой дисциплины, т.е. входное тестирование позволяет выявить готовность к усвоению новых знаний у учащихся.
<b>1.2</b>	Государственная политика в сфере общего образования РФ	Лекция  2 ч.	Лекция. Национальный проект образования. Федеральные проекты «Современная школа», «Учитель будущего». Приоритетные национальные задачи в сфере образования. Роль образовательной системы в общественном развитии. Федеральные государственные образовательные стандарты (ФГОС) общего образования нового поколения как основа развития системы образования. Самостоятельная работа. Приоритетные национальные задачи в сфере образования.
<b>1.3</b>	Нормативное регулирование в области информационной безопасности детей.	Лекция  2 ч,	Лекция: Стратегии национальной безопасности РФ, утвержденной Указом Президента РФ от 31.12.2015 N 683; Доктрина информационной безопасности РФ, утвержденной Указом Президента РФ от 05.12.2016 N 646; Основные направления государственной семейной политики, утвержденные Указом Президента РФ от 14.05.1996 N 712; Законом РФ от 27.12.1991 N 2124-1 "О средствах массовой информации" ; Статья 14 Федерального закона от 24.07.1998 N 124-ФЗ "Об основных гарантиях прав ребенка в РФ"; В Федеральном законе от 29.12.2010 N 436-ФЗ "О защите детей от информации, причиняющей вред их здоровью и развитию" ; Нормы, направленные на защиту детей от вредной информации, содержатся и в Федеральном законе от 13.03.2006 N 38-ФЗ "О рекламе".
<b>1.4</b>	Цифровая трансформация образования.	Практическое занятие  2 ч.	Практическое занятие. Анализ мер, реализуемых Правительством Российской Федерации в рамках Федерального проекта «Цифровая образовательная среда» национального проекта «Образование»: цели, задачи, основные мероприятия и результаты реализации. Самостоятельная работа. Перспективы развития цифрового образования в Российской Федерации. Реализация Указа Президента РФ «О национальных целях и стратегических задачах развития Российской Федерации на период до 2024 года».

<b>2.</b>	<b>Модуль 2. Планирование и организация деятельности по защите детей от угроз сети Интернет</b>		
<b>2.1</b>	Планирование и организация деятельности по обеспечению информационной безопасности в образовательной организации	Практическое занятие 2 ч.	Практическое занятие. Организация работы по использованию алгоритма безопасного использования сети Интернет: Актуальные угрозы информационной безопасности и защита информации при организации урока. Проведение аудита сайта на предмет возможности его использования в образовательной деятельности. Анализ типовых ошибок, меры по их предотвращению, устранению и защите образовательной организации от угроз сети Интернет Самостоятельная работа. Изучение учебных материалов по теме. Ответы на вопросы для самопроверки. Выполнение заданий в цифровой среде
<b>2.2</b>	Планирование и организация деятельности по выявлению угроз в сети Интернет	Практическое занятие 2 ч.	Практическое занятие. Организация работы по использованию алгоритма безопасного использования сети Интернет: Актуальные угрозы информационной безопасности и защита информации при организации урока. Проверка сайта на предмет возможности его использования в образовательной деятельности. Анализ типовых ошибок, меры по их предотвращению, устранению и защите образовательной организации от угроз сети Интернет. Самостоятельная работа. Изучение учебных материалов по теме.
<b>2.3</b>	Планирование и организация деятельности по защите от вредоносных программ	Практическое занятие 2 ч.	Практическое занятие. Организация защиты от вредоносного ПО - принципы работы, назначение. Организация противодействия распространённым ошибкам, создающим уязвимости для кибератак. Распространённые ошибки, приводящие к уязвимостям подключенных к сети Интернет устройств. Ответственность за нарушение правил сбора, хранения, использования и удаления охраняемой законом информации.
<b>2.4</b>	Планирование и организация деятельности по Безопасному использованию интеллектуальной собственности и предотвращению нарушений авторского права	Лекция 2 ч,	Лекция. Применимость в образовательной деятельности права на использование чужого контента, цитирование, консервативное авторское право, свободная лицензия, Creative Commons, правила использования свободной лицензии в образовании, виды лицензий. Организация работы по применению в образовательной организации алгоритма обеспечения максимальной защиты персональных устройств. Ассоциирование логотипов свободных лицензий с соответствующими им лицензионными условиями.
<b>2.5</b>	Планирование и организация деятельности по внедрению в практику	Практическое занятие 2 ч.	Практическое занятие. Применение в образовательной организации практических рекомендаций по защите от современных угроз – алгоритмов безопасного использования сети Интернет: – как использовать устройства при выходе в сеть Интернет; – меры предосторожности при использовании

	образовательной организации правил сетевой гигиены		электронной почты, мессенджеров и смс; безопасное скачивание файлов; – настройка безопасного поиска в поисковых системах, оценка и поиск безопасных сайтов через поисковые системы; удаление истории и файлов cookie из браузера. Самостоятельная работа. Изучение материалов по теме.
<b>Итоговая аттестация.</b>			
<b>4</b>	<b>Модуль 4. Итоговая аттестация</b>		
<b>4.1</b>	Выходное тестирование. Зачет.	Практическое занятие 2 ч .	Практическое занятие. Проверка уровня усвоения материала прослушанного курса.

### **3.Формы аттестации и оценочные материалы**

Формы аттестации – входное/выходное тестирование, текущий контроль (проверка усвоения учебного материала, регулярно осуществляемая на протяжении обучения), промежуточный контроль (оценивание качества освоения обучающимися отдельной части (модуля) или раздела, всего объема модулей) и итоговая аттестация по результатам освоения программы.

#### **1.Входное тестирование**

Входное тестирование - проводится по тесту, который включает 10 вопросов с выбором правильного варианта ответа из трех.

#### **Критерии оценивания входного тестирования**

За каждый правильный ответ слушатель получает 1 балл. Тест считается пройденным, если слушатель успешно прошел не менее 60% от предлагаемых заданий.

Интерпретация результатов:

- 60% выполненных заданий и выше – слушатель освоил содержание темы;
- менее 60% выполненных заданий – результат недостаточен, рекомендовано повторное прохождение темы.

*Примеры тестовых заданий.*

1.Основные источники угроз информационной безопасности:

- Хищение жестких дисков, подключение к сети, инсайдерство
- Перехват данных, хищение данных, изменение архитектуры системы
- Хищение данных, подкуп системных администраторов, нарушение регламента работы

2. Каким федеральным нормативно-правовым актом гарантируется общедоступность и бесплатность дошкольного, основного общего и среднего профессионального образования в государственных или муниципальных образовательных учреждениях и на предприятиях?

- Указ Президента Российской Федерации от 7 мая 2018 года №204 «О национальных целях и стратегических задачах развития Российской Федерации на период до 2024 года»

- Конституция Российской Федерации
- Национальный проект «Образование»

3. Что является методологической основой непрерывного образования и развития педагога?

- феноменологический подход
- экзистенциальная философия
- деятельностный подход

4. Кто в конечном счете несет ответственность за гарантии того, что данные классифицированы и защищены?

- Владельцы данных
- Пользователи
- Руководство

5. Как называется информация, которую следует защищать (по нормативам, правилам сети, системы)?

- Регламентированной
- Правовой
- Защищаемой

6. Основными объектами информационной безопасности являются:

- Компьютерные сети, базы данных
- Информационные системы, психологическое состояние пользователей
- Бизнес-ориентированные, коммерческие системы

7. Какая категория лиц является наиболее рискованной для работодателя с точки зрения вероятного мошенничества и нарушения безопасности?

- Хакеры
- Сотрудники
- Атакующие

8. Утечка информации в системе:

- это ситуация, которая характеризуется потерей данных в системе
- это ситуация, которая характеризуется изменением содержания информации
- это ситуация, которая характеризуется изменением формы информации

9. Что является одним из ведущих показателей уровня развитости современного общества?

- цифровизация основных социальных сфер
- социальные гарантии от государства
- показатель качества жизни

10. Когда получен спам по e-mail с приложенным файлом, следует:

- Прочитать приложение, если оно не содержит ничего ценного – удалить
- Удалить письмо с приложением, не раскрывая (не читая) его
- Сохранить приложение в парке «Спам», выяснить затем IP-адрес генератора спама

## **2. Выходное тестирование**

Выходное тестирование - проводится по тесту, он включает 10 вопросов с выбором правильного варианта ответа. Тест составлен из вопросов входного тестирования, промежуточного и текущего, а также вопросы по материалам изученных материалов.

### **Критерии оценивания выходного тестирования**

За каждый правильный ответ слушатель получает 1 балл. Тест считается пройденным, если слушатель успешно прошел не менее 60% от предлагаемых заданий).

*Примеры тестовых заданий.*

1. Какая классификация по возрасту не предусматривается законом №436-ФЗ о защите детей?

- 10 +
- 16 +
- 12 +

2. Ваши действия при получении письма от «Федеральной Налоговой Службы» с требованием привязать свою банковскую карту к portalу «Госуслуги»: Выберите один или несколько ответов:

- Проверите ссылку на портал Госуслуги, если ссылка открывается привяжете карту
- Письмо не открывать, сразу удалить
- Проверите адрес отправителя, сделаете звонок по указанному в письме номеру и выполните инструкции, полученные по телефону

3. Определите, какое поведение демонстрирует признаки игровой зависимости:

Выберите один или несколько ответов:

- Ребенок постоянно рассказывает как убивал гулей и альгулей, ходит в толстовке с надписью «Ведьмак 3»
- Ребенок постоянно играет в «стрелялку» на телефоне, при попытках его отвлечь ведет себя агрессивно Сообщает, что его сокомандники в игре «круче» чем одноклассники.
- Ребенок сообщает, что пропустил обед в школе, потому что карманные деньги потратил на скин в Доте 2

4. Заранее спланированная массовая акция офлайн, участники которой между собой незнакомы, но собираются в конкретном месте в условленное время, где недолго выполняют одно действие, после чего расходятся. Это –

- скулшутинг
- флешмоб
- зацепинг

5. Какие критерии станут определяющими для того, чтобы не использовать материалы из сети интернет учебном процессе?

- Нет возможности продемонстрировать учащимся материалы в первоисточнике.
- Информация является недостоверной. Она не подкреплена фактами
- Материал не содержит иллюстрации, видео и интерактивные вставки.

6. Выберите информацию, не являющуюся объектом персональных данных:

- Место регистрации и жительства гражданина
- Вес, рост и возраст гражданина
- Кличка домашнего животного гражданина

7. Ваши действия при получении сообщения от знакомого вам человека о том, что «Приюту требуется помощь, переведите деньги на банковский счет, животные страдают, счет идет на часы»

- Сообщение сразу удалить, отправителя заблокировать
- По ссылкам не переходить, деньги не переводить, переслать сообщение друзьям и коллегам, имеющим домашних животных
- Связаться с отправителем по каналу, отличному от того по которому пришло сообщение и уточнить причину отправки такого сообщения

8. Диггерство, зацепинг наказуемо законом?

- нет
- да
- закон находится в проекте

9. Ребенок сообщает, что когда одноклассники собираются на перемене, они выкрикивают в его адрес обидное прозвище. Ваши действия?

- Посоветуете ребенку избегать любого контакта с обидчиками, предложите заблокировать их всех в соцсетях
- Посоветуете ребенку игнорировать обращение по прозвищу и порекомендуете избегать открытой перепалки с толпой

- Посоветуете ребенку самому придумать обидные прозвища для всех обидчиков и объясните преимущества тактики «бей первым»

10. Ваши действия в случае, если вы получили письмо от неизвестного отправителя с темой «Важно!»:

- Удалить письмо, не открывая
- Проверить адрес отправителя, отправить письмо в архив
- Открыть письмо в «безопасном» режиме, проверить ссылки в тексте письма

### **3. Промежуточный контроль**

проводится по тесту, который включает 5 вопросов с выбором правильного варианта ответа из трех.

#### *Критерии оценивания промежуточного контроля*

Оценка «зачтено» выставляется, если слушатель курсов повышения квалификации прошел не менее 50% от предлагаемых заданий. Оценка «не зачтено» ставится, когда слушатель курсов повышения квалификации прошел не более 50% от предлагаемых заданий.

#### *Примеры тестовых заданий.*

1. Какие методы обучения входят в цифровую трансформацию образования?
  - смешанное обучение
  - взаимное обучение
  - лекции
2. Какая цифровая технология, согласно исследованию мониторинга цифровой трансформации, сегодня чаще всего используется в школах?
  - использование универсальных сервисов для решения задач управления
  - электронный журнал
  - использование социальных сетей и мессенджеров для управления школой
3. Какие из перечисленных технологий являются драйверами цифровой трансформации образования?
  - искусственный интеллект
  - книгопечатание
  - двигатель внутреннего сгорания
4. Какой процент школ планируется перевести к 2024 г. на безбумажные технологии управления?
  - 100%
  - 75%
  - 50%
5. Ваши действия в случае, если вы получили письмо от неизвестного отправителя с темой «Важно!»:

- Открыть письмо в «безопасном» режиме, проверить ссылки в тексте письма
- Удалить письмо, не открывая
- Ознакомиться с содержимым, скачать вложения и проверить их антивирусом

### **4. Итоговая аттестация. Зачёт.**

#### **Требования к итоговой аттестации**

Итоговая аттестация – оценка качества освоения слушателями дополнительной профессиональной программы повышения квалификации, соответствие окончательных результатов заявленным целям и планируемыми результатами обучения. Итоговая аттестация является обязательной для слушателей курсов, завершивших обучение по дополнительной профессиональной программе повышения квалификации. Продолжительность процедуры итоговой аттестации составляет 2 часа. Оценка качества обучения осуществляется на итоговых испытаниях в соответствии с разработанными критериями.

## Критерии оценивания итоговой аттестации

К итоговой аттестации, завершающей освоение дополнительной профессиональной программы, допускается слушатель курсов, успешно выполнивший все требования учебного плана, практико-ориентированные задания на практических занятиях, текущем контроле, а также выполнивший письменные практические задания по темам промежуточного контроля и выходного тестирования.

Оценка *«зачтено»* выставляется, если слушатель курсов повышения квалификации показывает усвоение узловых вопросов дополнительной профессиональной программы, глубокое знание структуры конкретных вопросов Программы, а также основного содержания и новаций теоретического материала, совершенствование/приобретение профессиональных навыков, демонстрирует отчетливое и свободное владение понятийным аппаратом программы, излагает ответ на вопрос аргументировано, четко, логически корректно, в ходе изложения материала приводит примеры, может применить теоретические знания для анализа конкретных ситуаций. Слушатель курсов повышения квалификации, показавший освоение планируемых результатов, предусмотренных Программой, сформированность профессиональной компетентности, способный к самостоятельному пополнению и обновлению знаний в ходе профессиональной деятельности получает оценку *«зачтено»*.

Оценка *«не зачтено»* ставится, когда слушатель курсов повышения квалификации не усвоил основного содержания тем данной Программы, с трудом применяет полученные теоретические знания для анализа конкретных ситуаций в процессе обучения и воспитания.

### *Примеры тестовых заданий.*

1. Заранее спланированная массовая акция офлайн, участники которой между собой незнакомы, но собираются в конкретном месте в условленное время, где недолго выполняют одно действие, после чего расходятся. Это -  
скулшутинг  
зацепинг  
флешмоб

2. Ваши действия при получении сообщения от знакомого вам человека о том, что «Приюту требуется помощь, переведите деньги на банковский счет, животные страдают, счет идет на часы»

- Сообщение сразу удалить, отправителя заблокировать

- Связаться с отправителем по каналу, отличному от того по которому пришло сообщение и уточнить причину отправки такого сообщения

- По ссылкам не переходить, деньги не переводить, переслать сообщение друзьям и коллегам, имеющим домашних животных

3. Ваши действия при получении письма от «Федеральной Налоговой Службы» с требованием привязать свою банковскую карту к portalу «Госуслуги»:

Выберите один или несколько ответов:

- Проверьте адрес отправителя, сделаете звонок по указанному в письме номеру и выполните инструкции, полученные по телефону

- Проверьте ссылку на портал Госуслуги, если ссылка открывается – привяжете карту

- Письмо не открывать, сразу удалить

4. Ваши действия в случае, если вы получили письмо от неизвестного отправителя с темой «Важно!»:

- Проверить адрес отправителя, отправить письмо в архив

- Открыть письмо в «безопасном» режиме, проверить ссылки в тексте письма
  - Удалить письмо, не открывая
5. Ребенок сообщает, что когда одноклассники собираются на перемене, они выкрикивают в его адрес обидное прозвище. Ваши действия?
- Посоветуете ребенку самому придумать обидные прозвища для всех обидчиков и объясните преимущества тактики «бей первым»
  - Посоветуете ребенку избегать любого контакта с обидчиками, предложите заблокировать их всех в соцсетях
  - Посоветуете ребенку игнорировать обращение по прозвищу и порекомендуете избегать открытой перепалки с толпой
6. Диггерство, зацепинг наказуемо законом?
- нет
  - закон находится в проекте
  - да
7. Определите, какое поведение демонстрирует признаки игровой зависимости: Выберите один или несколько ответов:
- Ребенок постоянно играет в «стрелялку» на телефоне, при попытках его отвлечь ведет себя агрессивно
  - Сообщает, что его сокомандники в игре «круче» чем одноклассники.
  - Ребенок постоянно рассказывает как убивал гулей и альгулей, ходит в толстовке с надписью «Ведьмак 3»
  - Ребенок сообщает, что пропустил обед в школе, потому что карманные деньги потратил на скин в Доте 2
- 8 Выберите информацию, не являющуюся объектом персональных данных:
- Место регистрации и жительства гражданина
  - Вес, рост и возраст гражданина
  - Кличка домашнего животного гражданина
9. Какая классификация по возрасту не предусматривается законом №436-ФЗ о защите детей?
- 12 +
  - 16 +
  - 10 +
10. Какие критерии станут определяющими для того, чтобы не использовать материалы из сети интернет учебном процессе?
- Материал не содержит иллюстрации, видео и интерактивные вставки.
  - Нет возможности продемонстрировать учащимся материалы в первоисточнике.
  - Информация является недостоверной. Она не подкреплена фактами

## **5.Организационно-педагогические условия реализации программы**

### **5.1 Учебно-методическое и информационное обеспечение программы**

#### **Рекомендованная литература**

##### **Нормативные документы**

1. Федеральный закон от 29.12.2010 N 436-ФЗ "О защите детей от информации, причиняющей вред их здоровью и развитию", (дата обращения 21.09.2021).
2. Федеральный закон от 27 июля 2006 г. N 149-ФЗ "Об информации, информационных технологиях и о защите информации".

3. Федеральный закон от 29.12.2012 N 273-ФЗ (ред. от 31.07.2020) "Об образовании в Российской Федерации", (дата обращения 21.09.2021).
4. Постановление Главного государственного санитарного врача Российской Федерации от 28.09.2020 № 28 "Об утверждении санитарных правил СП 2.4. 3648-20 "Санитарноэпидемиологические требования к организациям воспитания и обучения, отдыха и оздоровления детей и молодежи".
5. Методические рекомендации по ограничению в образовательных организациях доступа, обучающихся к видам информации.
6. Концепция информационной безопасности детей, утвержденной распоряжением Правительства РФ от 02.12.2015 N 2471. (дата обращения 21.09.2021).
7. Распоряжение Правительства РФ от 02.12.2015 N 2471-р "Об утверждении Концепции информационной безопасности детей" (дата обращения 21.09.2021).
8. Профессиональный стандарт «Педагог (педагогическая деятельность в дошкольном, начальном общем, основном общем, среднем общем образовании) (воспитатель, учитель)», приложение к приказу Минтруда РФ № 544н от 18.10.2013г., URL: [http://www.consultant.ru/document/cons\\_doc\\_LAW\\_155553/](http://www.consultant.ru/document/cons_doc_LAW_155553/) (дата обращения 21.09.2021)

#### Основная литература

1. Бирюков А.А. Информационная безопасность: защита и нападение. Москва: ДМК-Пресс, 2017.
2. Хломов К.Д., Давыдов Д.Г., Бочавер А.А. Кибербуллинг в опыте российских подростков. [Электронный ресурс] // Психология и право. 2019(9). No 2. С. 276-295. doi: 10.17759/psylaw.2019090219.
3. Международная информационная безопасность: Теория и практика: В трех томах: Учебник для вузов / Под общ. ред. А.В.Крутских. — М.: Издательство «Аспект Пресс», 2019.
4. Малюк А.А. Глобальная культура кибербезопасности // Горячая линия - Телеком. М., 2017. С. 308.
5. ЛеФевеер Л. Искусство объяснять. Как сделать так, чтобы вас понимали с полуслова; пер. с англ. Москва: Манн, Иванов и Фербер, 2018

#### Дополнительная литература

1. Ефимова, Л.Л. Информационная безопасность детей. Российский и зарубежный опыт. Монография. Гриф УМЦ «Профессиональный учебник». Гриф НИИ образования и науки. / Л.Л. Ефимова, С.А. Кочерга. — М.: ЮНИТИ, 2016. 239 с.
2. С. А. Петренко, В. А. Курбатов. Политики безопасности компании при работе в Интернет. Москва: ДМК-Пресс, 2016

#### Интернет-ресурсы

1. Курс «Безопасность в интернете» от Яндекса (дата обращения 21.09.2021)
2. Журнал для педагогов, психологов и родителей «Дети в информационном обществе » (дата обращения 21.09.2021)
3. Методическое пособие «Интернет: возможности, компетенции, безопасность». Солдатова Г., Зотова Е., Лебешева М., Шляпников

- В. URL: <http://detionline.com/internetproject/training-aids> (дата обращения 28.07. Интернета» 2020)
4. «Урок полезного и безопасного от компании МТС. URL: <http://detionline.com/mts/lessons> (дата обращения 21.09.2021)
5. Защита детей. Лаборатория Касперского URL: <https://kids.kaspersky.ru/>
6. Проект «Разбираем Интернет вместе с Google» URL: <http://www.razbiraeminternet.ru/> (дата обращения 21.09.2021)
7. PricewaterhouseCoopers: аналитический обзор по теме информационной безопасности (2018) URL: <https://www.pwc.ru/ru/publications/global-information-security-survey-2018.html> (дата обращения 21.09.2021).
8. «Исследования» от Mail.ru Group URL: <https://corp.mail.ru/ru/press/infograph/> (дата обращения 21.09.2021). 10. Мальцева В.А. Защита детей от кибербуллинга. вопросы уголовно-правового регулирования // научная электронная библиотека «Киберленинка» (Cyberleninka) (2019) URL: <https://cyberleninka.ru/article/n/zaschita-detey-ot-kiberbullinga-voprosy-ugolovnopravovogo-regulirovaniya> (дата обращения 21.09.2021)

## **5.2. Материально-технические условия обеспечения реализации программы**

Процесс реализации образовательной Программы обеспечивается необходимой материально-технической базой для проведения всех видов учебных занятий, предусмотренных учебным планом: лекционной, практической работы. Аудитория, используемая для реализации настоящей Программы, обеспечивается необходимым учебным оборудованием: компьютерами с мультимедийными проекторами, с доступом к Интернет-ресурсам, система управления курсами (электронное обучение) Moodle.

### **5.3. Кадровые условия**

Программа обеспечена преподавательским составом из числа кандидатов наук, доцентов, опытных старших преподавателей. Кадровый состав курсов соответствует лицензионному нормативу. Преподаватели курсов являются разработчиками ряда учебно-методических пособий, электронных методических материалов, методических рекомендаций. Курсы обладают высококачественным преподавательским составом, способным на высоком уровне решать задачи повышения квалификации. Педагогические работники повышают профессиональную квалификацию регулярно.

Условия реализации образовательного процесса являются достаточными для подготовки специалистов заявленного уровня.