Правительство Российской Федерации
Пермский филиал федерального государственного автономного образовательного учреждения высшего образования
"Национальный исследовательский университет
"Высшая школа экономики"
Факультет довузовской подготовки

С О Г Л А С О В А Н О
Заместитель директора ИРО ПК
_____ /Л.В. Волкова /
«___» _____ 2024 г.

У Т В Е Р Ж Д А Ю
Заместитель директора НИУ ВШЭ – Пермь
_____ /Е.П. Загороднова /
«___» _____ 2024 г.

«Профилактика правонарушений и преступлений в сети Интернет. Кибербезопасность детей и подростков»

дополнительная профессиональная программа повышения квалификации педагогических работников образовательных организаций Пермского края
(36 часов)

Пермь, 2024

Разработчики программы:

Фамилия, инициалы	**Место работы, должность, ученая степень, ученое звание**
Гангнус Н.А.	Пермский государственный гуманитарно-педагогический университет, доцент кафедры педагогики и психологии, кандидат педагогических наук
Кылосов Д.В.	Пермская региональная общественная организация «ПравДА вместе», IT-специалист, эксперт-аналитик Ресурсного центра профилактики деструктивного влияния информации на несовершеннолетних в Пермском крае
Скорнякова Анна Юрьевна	Пермский государственный гуманитарно-педагогический университет, декан математического факультета, доцент кафедры высшей математики и методики обучения математике, кандидат педагогических наук
Хан О.А.	Пермская региональная общественная организация «ПравДА вместе», педагог-психолог, эксперт-аналитик Ресурсного центра профилактики деструктивного влияния информации на несовершеннолетних в Пермском крае
Уточкин Ю.А.	Пермский государственный медицинский университет, доцент кафедры общественного здоровья и здравоохранения, кандидат медицинских наук

Рецензенты программы:

Фамилия, инициалы	**Место работы, должность, ученая степень, ученое звание**
Тимкина Ю.Ю.	канд. пед. наук, доцент кафедры иностранных языков и связей с общественностью ПНИПУ

1. Характеристика программы

1.1. Цель реализации программы: совершенствование профессиональных компетенций слушателей в сфере профилактики правонарушений и преступлений в сети Интернет и кибербезопасности детей и подростков.

1.2. Планируемые результаты обучения:
Профессиональный стандарт Педагог (педагогическая деятельность в сфере дошкольного, начального общего, основного общего, среднего общего образования) (воспитатель, учитель), утверждённый приказом Министерства труда и социальной защиты РФ от 18 октября 2013 г. N 544н):

Трудовая функция	Трудовое действие	Знать	Уметь
Общепедагогическая функция. Обучение.	Формирование навыков, связанных с информационно-коммуникационными технологиями.	Сущность процесса обеспечения информационной безопасности в сети Интернет в рамках реализации профессионально-педагогической деятельности; особенности планирования и организации деятельности по внедрению в практику образовательной организации правил сетевой гигиены; виды, признаки киберугроз и основные способы обеспечения кибербезопасности детей и подростков; способы противодействия деструктивному влиянию информации на детей в сети Интернет.	Применять в образовательной деятельности меры по профилактике правонарушений и преступлений в сети Интернет, меры по обеспечению кибербезопасности детей и подростков.
Воспитательная деятельность.	Регулирование поведения обучающихся для обеспечения безопасной образовательной среды. Реализация современных, в том числе интерактивных, форм и методов воспитательной работы, использование их как на занятии, так и во внеурочной деятельности.		
Развивающая деятельность.	Оценка параметров и проектирование психологически безопасной и комфортной образовательной среды, разработка программ профилактики различных форм насилия в школе.		

Приказ Минздравсоцразвития РФ от 26.08.2010 N 761н «Об утверждении Единого квалификационного справочника должностей руководителей, специалистов и служащих, раздел "Квалификационные характеристики должностей работников образования»:

Должностные обязанности по ЕКС	Знать	Уметь
Преподаватель	Сущность процесса обеспечения информационной	Применять в образовательной деятельности меры по
Обеспечивает охрану жизни и здоровья обучающихся во время		

образовательного процесса. Вносит предложения по совершенствованию образовательного процесса в образовательном учреждении.	безопасности в сети Интернет в рамках реализации профессионально-педагогической деятельности; особенности планирования и организации деятельности по внедрению в практику образовательной организации правил сетевой гигиены; виды, признаки киберугроз и основные способы обеспечения кибербезопасности детей и подростков; способы противодействия деструктивному влиянию информации на детей в сети Интернет.	профилактике правонарушений и преступлений в сети Интернет, меры по обеспечению кибербезопасности детей и подростков.
Методист (включая старшего)		
Обеспечивает охрану жизни и здоровья обучающихся во время образовательного процесса. Вносит предложения по совершенствованию образовательного процесса в образовательном учреждении.		

1.3. Категория слушателей: учителя НОО, учителя ООО, учителя СОО, преподаватели СПО, педагоги-наставники, педагоги-методисты.

1.4. Форма обучения: очно-заочная, с применением дистанционных образовательных технологий.

1.5. Срок освоения программы: трудоемкость программы 36 учебных часов, в т.ч. 22 часа контактной работы с преподавателем. Для всех видов учебной нагрузки академический час устанавливается продолжительностью 45 минут.

2. Содержание программы

2.1. Содержание программы в разрезе разделов (модулей), тем, видов учебных занятий, форм контроля

№ п/п	Наименование разделов (модулей) и тем	Всего часов	Виды учебных занятий, учебных работ		Самостоятельная работа, час	Формы контроля
			Лекции, час	Практические (интерактивные) занятия, час		
1.	Информационная безопасность в сети Интернет как педагогическая задача.	2	1	0	1	
2.	Кибербезопасность детей и подростков: цифровая гигиена, цифровые следы, цифровая репутация.	6	1	3	2	

3.	Нормативно-правовое регулирование сферы кибербезопасности детей и подростков.	2	1	0	1	
4.	Современные социальные киберугрозы в молодежной среде: влияние и маркеры их проявления.	6	0	4	2	Практическое задание
5.	Манипуляция общественным сознанием в информационном пространстве: способы защиты детей и подростков.	2	0	2	0	
6.	Деструктивное влияние информации на детей в сети Интернет: угрозы и способы противодействия им.	6	1	3	2	
7.	Террористические и экстремистские проявления в информационной среде: маркеры вовлечения несовершеннолетних, профилактика в условиях образовательной организации.	4	0	2	2	
8.	Реализация государственной политики в сфере воспитания на уроках и во внеурочной деятельности.	2	0	2	0	
9.	Использование оборудования и цифровых ресурсов в обучении и воспитании детей и подростков.	2	0	0	2	
10.	Оказание первой помощи в условиях образовательной организации.	2	0	0	2	
11.	Итоговая аттестация обучающихся.	2	0	2	0	зачет

	Итого:	36	4	18	14	

2.2. Рабочая программа

Тема 1. Информационная безопасность в сети Интернет как педагогическая задача.

Понятие информационной безопасности в сети Интернет. Классификация угроз информационной безопасности. Актуальные угрозы информационной безопасности и защита информации при организации учебной деятельности в образовательной организации.

Теория: интерактивные лекции с презентацией.

Самостоятельная работа: анализ средств обеспечения информационной безопасности в образовательной организации.

Тема 2. Кибербезопасность детей и подростков: цифровая гигиена, цифровые следы, цифровая репутация.

Понятие «цифровая гигиена». Правила безопасного поведения субъектов образовательного процесса в сети Интернет. Технические аспекты обеспечения кибербезопасности в образовательной организации. Планирование и организация деятельности по внедрению в практику образовательной организации правил сетевой гигиены. Кибербезопасность и информационная безопасность. Принципы психического и эмоционального благополучия при использовании цифровых технологий. Понятие «цифровые следы», понятие «цифровая репутация». Виды цифровых следов, «цифровое облако», личная и публичная информация. Формирование цифровой репутации в период развития цифрового мира. Угрозы цифровой репутации. Последствия негативного цифрового следа.

Теория: интерактивные лекции с презентацией.

Практика: анализ способов и методов обеспечения цифровой гигиены в современной образовательной организации. Планирование и организация деятельности по внедрению в практику образовательной организации правил сетевой гигиены.

Самостоятельная работа: чек-лист правил кибергигиены (цифровой гигиены) для обучающихся.

Тема 3. Нормативно-правовое регулирование сферы кибербезопасности детей и подростков.

Принципы защиты информации в России, законодательство в сфере формирования безопасной информационной среды. Виды информации, причиняющие вред здоровью и развитию несовершеннолетних, возрастные ограничения. Механизм правовой оценки информации по критериям причинения вреда жизни и здоровью детей и подростков. Разграничение полномочий субъектов профилактики по защите детей и подростков от информации, причиняющей вред их здоровью и развитию.

Теория: интерактивные лекции с презентацией.

Самостоятельная работа: анализ основных аспектов Федерального закона №436 «О защите детей от информации, причиняющей вред их здоровью и развитию».

Тема 4. Современные социальные киберугрозы: влияние и маркеры их проявления.

Виды киберугроз. Социальные киберугрозы. Понятие противозаконных и агрессивно-хулиганских субкультур в России, виды (офники, АСАВ, андерграунд). Маркеры выявления угроз. Противозаконные субкультуры, их криминальные проявления (дроппинг, курьерство). Иные околопротивозаконные явления в детско-молодежной среде, границы юридической ответственности. Цифровой профиль школьника в социальной сети. Элементы формирования: аватар профиля, данные о себе, доменное имя, фото и видео контент, посты и репосты, музыкальный контент, использование детьми и подростками цифрового контента из групп (сообществ, пабликов) цифрового пространства. Влияние киберугроз на детей и подростков.

Практика: анализ признаков и проявлений социальных киберугроз и их влияние на несовершеннолетних.

Самостоятельная работа: решение кейса «Выявление признаков социальных киберугроз в образовательной организации».

Тема 5. Манипуляция общественным сознанием в информационном пространстве: способы защиты детей и подростков.

Понятие «общественное сознание» и влияние на него через цифровую среду. Механизм манипуляции детским сознанием. Средства манипуляции в информационном пространстве. Вербовка как метод информационно-психологического влияния на детей и подростков. Способы защиты от манипуляции детским сознанием.

Практика: анализ способов защиты детей и подростков от манипуляции сознания.

Тема 6. Деструктивное влияние информации на детей в сети Интернет: угрозы и способы противодействия им.

Деструктивный контент. Вовлечение детей и подростков в деструктивное поведение в сети Интернет. Воронка вовлечения детей и подростков в деструктивные сообщества. Механизм «Окна Овертона», юридические и психологические последствия для отдельного ребенка и для общественного сознания в целом. Способы противодействия угрозам в условиях образовательной организации.

Теория: интерактивные лекции с презентацией.

Практика: анализ способов противодействия деструктивному влиянию информации в сети Интернет на детей и подростков в условиях образовательной организации.

Самостоятельная работа: решение кейса «Анализ маркеров вовлечения несовершеннолетних в деструктивные сообщества».

Тема 7. Террористические и экстремистские проявления в информационной среде: маркеры вовлечения несовершеннолетних, профилактика в условиях образовательной организации.

Роль школы и общественных организаций в воспитательной работе обучающихся. Формирование антитеррористической грамотности обучающихся. Маркеры проявления террористических и экстремистских угроз в информационном пространстве.

Практика: анализ мероприятий, направленных на профилактику террористических и экстремистских проявлений, действий педагогических работников по обеспечению информационной безопасности обучающихся.

Самостоятельная работа: анализ мер по профилактике террористических и экстремистских проявлений в информационной среде в условиях конкретной образовательной организации.

Тема 8. Реализация государственной политики в сфере воспитания на уроках и во внеурочной деятельности.

Государственная политика в сфере воспитания и ее реализация в образовательной организации: управленческие решения. Значимость вопросов усиления воспитательного потенциала педагогической деятельности в образовательном процессе. Лично-развивающая стратегия воспитания.

Практика: анализ проблем в организации воспитательного процесса в деятельности современного педагога.

Тема 9. Использование оборудования и цифровых ресурсов в обучении и воспитании детей и подростков.

Интерактивные методы в образовательном и воспитательном процессе. Особенности внедрения и применения цифровых сервисов и решений для организации урочной и внеурочной деятельности обучающихся.

Самостоятельная работа: анализ возможности применения в своей образовательной организации цифровых образовательных ресурсов и цифровых решений для организации урочной и внеурочной деятельности обучающихся.

Тема 10. Оказание первой помощи в условиях образовательной организации.

Самостоятельная работа: изучение принципов и правил оказания первой помощи в условиях образовательной организации, основных приемов оказания доврачебной медицинской помощи. Рекомендована отработка правил и приемов оказания первой помощи.

Итоговая аттестация обучающихся.

Выполнение итоговой зачетной работы в форме выполнения итогового теста по теме «Безопасная образовательная среда: профилактика правонарушений в информационном пространстве» и решения кейса «Анализ профиля несовершеннолетнего в социальной сети».

3. Формы аттестации и оценочные материалы

Контрольные мероприятия проводятся в ходе лекций и практических занятий – как результат обратной связи со слушателями. Для самоконтроля слушатели выполняют/получают ссылки на электронные ресурсы, а также дополнительные материалы в виде приложений и презентаций на заданные темы.

Входной, промежуточный контроль не предусмотрен.

Текущий контроль

Форма текущего контроля.

Практическое задание.

Описание, требования к выполнению.

После изучения темы 4 «Современные социальные киберугрозы: влияние и маркеры их проявления» слушателям предлагается выполнить практическое задание. Слушатели анализируют предложенные ситуационные задачи и определяют возможные маркеры киберугрозы. Слушатели предоставляют выполненное практическое задание преподавателю для дальнейшей оценки. Формат выполненной работы – текстовый (не более 2 страниц).

Количество попыток: не ограничено.

Примеры заданий.

Проанализируйте предложенную ситуационную задачу, выявите наличие/ отсутствие признаков социальных киберугроз/ определите маркеры, которые свидетельствуют о наличии киберугрозы. Представьте свои выводы.

Критерии оценивания.

Зачет/ не зачет. Задание оценивается преподавателем, в случае необходимости дорабатывается слушателем с учетом замечаний.

Итоговая аттестация

Форма итоговой аттестации.

По завершении программы слушатели проходят одно аттестационное испытание в форме выполнения итоговой зачетной работы. Зачет проводится в форме выполнения итогового теста по теме «Безопасная образовательная среда: профилактика правонарушений в информационном пространстве» и решения кейса «Анализ профиля несовершеннолетнего в социальной сети».

Описание, требования к выполнению.

На проведение итоговой аттестации отводится 2 аудиторных часа.

Итоговая аттестация состоит из двух частей. Первая часть: выполнение итогового теста на 10 вопросов. Вторая часть: решение кейса с последующим обсуждением.

Примеры заданий (примерное содержание итоговой работы).

Тест:

1. Какие проблемы решаются с помощью кибергигиены?
а) Нарушение безопасности, потеря данных.
б) Устаревшее программное обеспечение.
в) Устаревший антивирус.
г) Все выше перечисленное.

2. Выберите основные формы педагогической профилактики правонарушений несовершеннолетних:
1) Социально-педагогическая диагностика;
2) Информационно-просветительская работа с родителями;
3) Информационно-просветительская работа с обучающимися;
4) Социально-профилактическая работа;
5) Все вышеперечисленное.

3. Способами распространения идеологии деструктивизма и экстремизма в молодёжной среде могут стать:
1) Социальные сети и информационные порталы;
2) Интернет-сообщества, тематические форумы;
3) Интернет-игры.

4. Основной задачей деятельности по профилактике безнадзорности и правонарушений несовершеннолетних не является:
1) Пополнение профессионального портфолио педагога;
2) Предупреждение безнадзорности, беспризорности, правонарушений и антиобщественных действий несовершеннолетних, выявление и устранение причин и условий, способствующих этому;
3) Создание системы воспитательной работы, направленной на профилактику безнадзорности и правонарушений несовершеннолетних;
4) Социально-педагогическая реабилитация несовершеннолетних, находящихся в социально опасном положении.

5. Информационная безопасность детей - это:
1) Это 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;
2) Это защита компьютеров, сетей, программных приложений, критически важных систем и данных от потенциальных цифровых угроз.

6. Сопоставьте виды кибербуллинга и его характеристики:
1. Фишинг А
2. Вишинг Б
3. "Липовые акции"
4. Фишинг-атаки
5. Ложная блокировка

А. Заманивание пользователя на поддельный сайт, с целью перехватить данные пользователя (данные карты, логин, пароль сайта-оригинала и т.п.);

Б. Мошенничество с помощью телефона. Цель – выманить платежные данные, с помощью которых можно украсть деньги с карты или кошелька. Часто дополнительно присылается СМС со ссылкой, которая ведет на фишинговый сайт.

В. Пользователь может получить сообщение (по телефону, почте или SMS), что выиграл некий приз, а для его получения необходимо «уплатить налог», «оплатить доставку» или просто пополнить какой-то счет);

В. Пользователю на электронную почту поступают всплывающие сообщения и ссылки на фишинговые веб-сайты, с целью обманным путем выявить у получателя личную информацию, часто финансового характера.

Г. При попытке зайти в социальную сеть появляется баннер/экран/картинка, где подробно расписан вариант «спасения» от блокирования страницы, который включает отправку SMS на «короткий» номер или введение кода подтверждения. В первом случае происходит разовое списание денег, а во втором оформляется ежедневная подписка на какую-либо платную услугу.

7. Чем опасны социальные сети?

1) Личная информация может быть использована кем угодно в разных целях
2) При просмотре неопознанных ссылок компьютер может быть взломан
3) Все вышеперечисленное верно

8. Как защититься ото всех технологических угроз сети Интернет? (выбор одного правильного ответа):

1) Установить на все свои устройства комплексные системы защиты с антивирусом, спам-фильтром, сканером трафика, брандмауэром и выставить все установки в режим максимально возможной защиты;

2) Достаточно поставить антивирус и соблюдать правила цифровой гигиены;

3) Единственный способ защититься ото всех угроз сети Интернет – никогда не подключаться к сети Интернет. Других гарантированных способов не существует;

4) Выходить в интернет из внутренних корпоративных сетей – тогда между пользователем и злоумышленниками стоит как минимум IT персонал интернета.

9. К информации, запрещенной для распространения среди детей, относится информация:

1) Побуждающая детей к совершению действий, представляющих угрозу их жизни и (или) здоровью, в том числе к причинению вреда своему здоровью, самоубийству; способная вызвать у детей желание употребить наркотические средства, психотропные и (или) одурманивающие вещества, табачные изделия, алкогольную и спиртосодержащую продукцию, пиво и напитки, изготавливаемые на его основе, принять участие в азартных играх, заниматься проституцией, бродяжничеством или попрошайничеством;

2) Вызывающая у детей страх, ужас или панику, в том числе представляемая в виде изображения или описания в унижающей человеческое достоинство форме ненасильственной смерти, заболевания, самоубийства, несчастного случая, аварии или катастрофы и (или) их последствий;

3) Содержащая бранные слова и выражения, не относящиеся к нецензурной брани.

10. Какие рекомендации по информационной безопасности руководитель может дать родителям (законным представителям) детей 9-12 лет? (выбор одного правильного ответа):

1) Регулярно разговаривайте с ребенком о том, что происходит в его «онлайн-жизни»;

2) Установите систему «Родительского контроля» на устройствах, с которых ребенок будет выходить в Интернет;

3) Установите программу-шпион на устройствах ребенка для скрытого наблюдения за его действиями в интернете;

4) Запретите ребенку иметь аккаунты в социальных сетях.

Кейс:

Слушателям предлагаются несколько профилей несовершеннолетних в социальной сети «Вконтакте» (возможна работа в группах до 5-ти человек). Необходимо:

1. Проанализировать профиль несовершеннолетнего: аватар профиля, данные о себе, доменное имя, фото и видео контент, посты и репосты, музыкальный контент, использование детьми и подростками цифрового контента из групп (сообществ, пабликов) цифрового пространства.
2. Сделать выводы о безопасности профиля/ небезопасности. Обосновать свои выводы на конкретных примерах.
3. Представить данную информацию с последующим обсуждением в группе.

Критерии оценивания.

Оценка за зачет выставляется по 10-ти балльной шкале. Удовлетворительными (зачет сдан) считаются оценки от 4 баллов включительно и выше, неудовлетворительными (зачет не сдан) – 4 балла и ниже. За каждый верный ответ в тесте ставится 1 балл.

Критерии оценивания:

Критерии	Параметры	Количество баллов
Часть 1 «Тест»	Количество верно выполненных заданий от 5 до 7	2
	Количество верно выполненных заданий от 8 до 10	4
Часть 2 «Кейс»	Полнота решения кейса	1
	Доказательность и убедительность решения	1
	Наличие собственных взглядов на выявленные проблемы	2
	Полнота, всесторонность и обоснованность выводов	2
Итого		10 баллов

4. Организационно-педагогические условия реализации программы

4.1. Организационно-методическое и информационное обеспечение программы.

Нормативные документы:

1. Федеральный закон от 29.12.2012 № 273-ФЗ «Об образовании в Российской Федерации»;
2. Федеральный закон от 31 июля 2020 г. № 304-ФЗ «О внесении изменений в Федеральный закон «Об образовании в Российской Федерации» по вопросам воспитания обучающихся»;
3. Постановление Правительства РФ от 16 ноября 2020 г. № 1836 «О государственной информационной системе «Современная цифровая образовательная среда»;
4. Распоряжение Правительства РФ от 22 марта 2017 г. № 520-р «Об утверждении Концепции развития системы профилактики безнадзорности и правонарушений несовершеннолетних на период до 2025 года»;
5. Распоряжение Правительства Российской Федерации от 29.05.2015 № 996-р «Стратегия развития воспитания в Российской Федерации на период до 2025 года».
6. Приказ Минпросвещения России от 31.05.2021 № 286 «Об утверждении федерального государственного образовательного стандарта начального общего образования»;
7. Приказ Минпросвещения России от 18.07.2022 № 569 «О внесении изменений в федеральный государственный образовательный стандарт начального общего образования, утвержденный приказом Министерства просвещения Российской Федерации от 31 мая 2021 г. № 286».

8. Приказ Минпросвещения России от 31.05.2021 № 287 «Об утверждении федерального государственного образовательного стандарта основного общего образования».
9. Приказ Минпросвещения России от 18.07.2022 № 568 «О внесении изменений в федеральный государственный образовательный стандарт основного общего образования, утвержденный приказом Министерства просвещения Российской Федерации от 31 мая 2021 г. № 287».
10. Приказ Минобрнауки России от 17.05.2012 № 413 «Об утверждении федерального государственного образовательного стандарта среднего общего образования».
11. Приказ Минпросвещения России от 12.08.2022 № 732 «О внесении изменений в федеральный государственный образовательный стандарт среднего общего образования, утвержденный приказом Министерства образования и науки Российской Федерации от 17 мая 2012 г. № 413».
12. Приказ Министерства здравоохранения и социального развития Российской Федерации от 26 августа 2010 г. № 761н «Об утверждении единого квалификационного справочника должностей руководителей, специалистов и служащих, раздел «квалификационные характеристики должностей работников образования».
13. Профессиональный стандарт Педагог (педагогическая деятельность в сфере дошкольного, начального общего, основного общего, среднего общего образования) (воспитатель, учитель), утверждённый приказом Министерства труда и социальной защиты РФ от 18 октября 2013 г. N 544н).

Литература

1. Дубов С.С., Линьков В.В., Карбаинова М.А. Информационная безопасность ребенка в цифровом пространстве Российской Федерации. Russian Technological Journal. 2019; 7(4): С. – 21-30.
2. Клименко И.С. Информационная безопасность и защита информации: модели и методы управления / И.С. Клименко. М.: Инфра-М, 2020. – 180 с.
3. Мы в ответе за цифровой мир. Профилактика деструктивного поведения подростков и молодежи в Интернете: учебно-методическое пособие / Г. У. Солдатова, А. А. Дренёва, С.В. Чигарькова, С. Н. Илюхина. М.: Когито-Центр, 2019. – 176 с.
4. Райтман М.А. Информационная безопасность для пользователя. Правила самозащиты в Интернете / М.А. Райтман. М.: БВХ, 2023. – 400 с.
5. Шек Е.Д. Повышение качества образования посредством использования новых информационных технологий / Е.Д. Шек, А.Э. Григорян А.Э. // Влияние новейших технологий, СМИ, Интернета на образование, язык и культуру: сб. ст. по материалам Всерос. науч.-практ. конф. М., 2020. – С. 268-273.

Профессиональные базы данных, информационно-справочные системы

1. Электронно-библиотечная система Юрайт https://biblio-online.ru/
2. Научная электронная библиотека https://www.elibrary.ru/
3. Российская электронная школа https://resh.edu.ru/

Интернет-источники

1. 15 правил безопасного поведения в интернете https://www.ucheba.ru/project/websafety
2. Protect: безопасность в интернете https://browser.yandex.ru/help/security/protection.html
3. Информационная безопасность ребенка в цифровом пространстве Российской Федерации https://www.rtj-mirea.ru/jour/article/view/160
4. Информационная безопасность детей и подростков https://www.youtube.com/watch?v=U8OMAuPWPE8
5. Информационная безопасность школьников в сети Интернет: проблемы и пути решения https://cyberleninka.ru/article/n/informatsionnaya-bezopasnost-shkolnikov-v-seti-internet-problemy-i-puti-resheniya

6. Как научить детей кибербезопасности https://www.kaspersky.ru/resource-center/preemptive-safety/cybersecurity-for-kids
7. Меры профилактики преступлений, совершаемых в Интернете, среди несовершеннолетних лиц https://cyberleninka.ru/article/n/mery-profilaktiki-prestupleniy-sovershaemyh-v-internete-sredi-nesovershennoletnih-lits
8. Методические рекомендации для несовершеннолетних, родителей (законных представителей) несовершеннолетних, наглядные информационные материалы по безопасному использованию сети «Интернет» в целях предотвращения преступлений, совершаемых с ее использованием, как самими несовершеннолетними, так и в отношении них https://docs.edu.gov.ru/document/

4.2. Материально-технические условия реализации программы

Для проведения занятий созданы условия, обеспечивающие реализацию дополнительной профессиональной образовательной программы:
– информирование слушателей о сроках, учебном плане, организационных аспектах проведения курсов;
– предоставление современного учебного оборудования (мультимедийные проекторы, интерактивные доски, документ-камера, микрофон и т.д.);
– исчерпывающий набор дидактических, учебно-методических материалов, из расчета по одному полному комплекту на каждого слушателя;
– возможность пользования библиотекой с необходимым количеством учебной и методической литературы в печатном и электронном виде по всем темам обучения; читальным залом;
– предоставление слушателю материалов на бумажном носителе и презентационных материалов в электронном виде.
– предоставление слушателю доступа в LMS (Learning Management System) – системе, для организации учебного процесса в цифровой среде.

Раздел 5. Требования к отсроченным результатам обучения

5.1. Требования к отсроченным результатам

В результате освоения программы обучающийся должен приобрести следующие знания и умения, необходимые для качественного изменения компетенций:

обучающийся должен знать: сущность процесса обеспечения информационной безопасности в сети Интернет в рамках реализации профессионально-педагогической деятельности; особенности планирования и организации деятельности по внедрению в практику образовательной организации правил сетевой гигиены; виды, признаки киберугроз и основные способы обеспечения кибербезопасности детей и подростков; способы противодействия деструктивному влиянию информации на детей в сети Интернет, основные способы профилактики террористических и экстремистских проявлений в информационной образовательной среде; основы государственной политики в сфере воспитания; правила оказания первой помощи;

обучающийся должен уметь: применять в образовательной деятельности меры по профилактике правонарушений и преступлений в сети Интернет, меры по обеспечению кибербезопасности детей и подростков, оказывать доврачебную помощь;

обучающийся должен владеть: способами профилактики правонарушений и преступлений в сети Интернет, навыками обеспечения кибербезопасности детей и подростков в образовательной организации.

5.2. Оценочные материалы для отслеживания отсроченных результатов

Отслеживание и оценка отсроченного результата освоения программы производится с использованием «Листа оценки». «Лист оценки» предназначен для комплексной оценки компетенций, приобретаемых в результате обучения по программе повышения квалификации, с указанием подтверждающих материалов. Является вкладышем в портфолио учителя и служит для мониторинга со стороны структур управления и самоконтроля.

«Лист оценки» заполняется по мере приобретения опыта работы, и проверяется через полгода и (или) год после окончания процесса обучения. Может заполняться в процессе всей деятельности педагогического работника, дополняться другими листами оценки по новым курсам (новым компетенциям). Работа с таким материалом со стороны учителя позволяет создать пул (портфель) компетенций для упрощения аспектов профессиональной деятельности. Ведётся в электронном виде.

Возможные варианты оценки отсроченных результатов: самообследование, внутренняя оценка, внешняя оценка с привлечением экспертов.

Форма «Лист оценки»

Ф.И.О. (слушателя) _____

Образовательное учреждение _____

Курсы повышения квалификации_____

Период обучения: _____

Организатор курсов: _____

Итоговая оценка (экзамен, зачёт, проект):

Формируемые компетенции	**Критерии оценки/ Подтверждающие материалы**	**Результат оценки**
Владеет способами профилактики правонарушений и преступлений в сети Интернет, навыками обеспечения кибербезопасности детей и подростков в образовательной организации.	Внедрен комплекс мер в образовательной организации по профилактике безопасности правонарушений и преступлений в сети Интернет на нормативно-правовом и административно-организационном уровнях.	Внедрен/ не внедрен
	и (или)	
	Внедрен комплекс мер в образовательной организации по обеспечению кибербезопасности обучающихся.	Внедрен/ не внедрен
	и (или)	
	Проведены внеклассные мероприятия для детей и подростков разных возрастных групп по кибербезопасности, направленные на профилактику правонарушений и преступлений в сети Интернет.	Проведены/ Не проведены

Степень влияния освоенной слушателями программы повышения квалификации на профессиональную деятельность оценивается по результатам оценки отсроченного результата освоения программы повышения квалификации: положительная оценка влияния содержания и форм обучения на принятие идей, концепций, решений, представленных в ходе обучения, как руководства для осуществления профессиональной деятельности – выполнение 2 и более критериев оценки (с предоставлением подтверждающих материалов).