Государственное бюджетное учреждение
дополнительного профессионального образования
«Санкт-Петербургский центр оценки качества образования
и информационных технологий»

МЕТОДИЧЕСКИЕ РЕКОМЕНДАЦИИ
по актуализации (проектированию) содержания программ повышения квалификации педагогических и руководящих работников образовательных организаций по вопросам организации информационной безопасности обучающихся при работе в сети Интернет

Авторы:

Дорофеева Татьяна Владимировна, заведующий сектором отдела учебно-методической работы ГБУ ДПО “СПбЦОКОиИТ”.
Туманов Иван Анатольевич, методист отдела учебно-методической работы ГБУ ДПО “СПбЦОКОиИТ”.

Санкт-Петербург
2018

1. Общие положения

Методические рекомендации по актуализации (проектированию) содержания программ повышения квалификации педагогических и руководящих работников образовательных организаций по вопросам организации информационной безопасности обучающихся при работе в сети Интернет (далее – Методические рекомендации) разработаны на основе положений:

1) Федерального закона от 29.12.2010 г. N 436-ФЗ “О защите детей от информации, причиняющей вред их здоровью и развитию”;

2) Концепции информационной безопасности детей, утвержденной распоряжением Правительства Российской Федерации от 2 декабря 2015 г. № 2471-р;

3) Рекомендаций парламентских слушаний “Актуальные вопросы обеспечения безопасности и развития детей в информационном пространстве”, прошедших в Совете Федерации 17 апреля 2017 г.;

4) Письма Минобрнауки России от 14.05.2018 г. № 08-1184 “О направлении информации” (вместе с “Методическими рекомендациями о размещении на информационных стендах, официальных интернет-сайтах и других информационных ресурсах общеобразовательных организаций и органов, осуществляющих управление в сфере образования, информации о безопасном поведении и использовании сети “Интернет”).

Методические рекомендации направлены на повышение качества проектирования содержания дополнительных профессиональных программ повышения квалификации руководящих и педагогических работников образовательных организаций в части организации деятельности по профилактике вовлечения детей и молодежи в криминальную, в том числе экстремистскую, деятельность посредством сети Интернет (далее - обеспечение безопасного пребывания обучающихся в сети Интернет).

Методические рекомендации позволят государственным образовательным учреждениям дополнительного профессионального образования актуализировать содержание программ повышения квалификации по вопросам организации деятельности руководящих и педагогических работников ОО в направлении обеспечения безопасного пребывания обучающихся в сети “Интернет”.

Методические рекомендации носят рекомендательный характер и содержат:

- Рекомендации по актуализации (проектированию) содержания программ повышения квалификации педагогических работников образовательных организаций.
- Рекомендации по актуализации (проектированию) содержания программ повышения квалификации руководящих работников образовательных организаций.
- Рекомендации по выбору форм и технологий организации образовательной деятельности слушателей.
- Рекомендации по разработке программы внеурочной деятельности для обучающихся основной и средней школы.
- Ресурсы сети Интернет для использования в работе по обеспечению безопасного пребывания обучающихся в сети Интернет (приложение № 1).
- Программное обеспечение для для использования в работе по обеспечению безопасного пребывания обучающихся в сети Интернет (приложение № 2).
- Рекомендации законодательных и исполнительных органов власти РФ по организации работы по обеспечению безопасного пребывания обучающихся в сети Интернет (приложение № 3).
- Методические материалы для организации работы по обеспечению безопасного пребывания обучающихся в сети Интернет в образовательных организациях (приложение № 4).
- Учебно-методические материалы для обеспечения реализации программы повышения квалификации для педагогических и руководящих работников образовательных организаций (приложение № 5).

2. Рекомендации по актуализации (проектированию) содержания программ повышения квалификации педагогических работников образовательных организаций

При актуализации (проектировании) содержания программ повышения квалификации педагогических работников образовательных организаций по вопросам обеспечения безопасного пребывания обучающихся в сети Интернет в их содержание могут быть включены следующие темы:

- Информационная безопасность в сети Интернет.
- Государственное регулирование в сфере обеспечения информационной безопасности обучающихся при доступе к сети Интернет.
- Угрозы информационной безопасности в сети Интернет.
- Меры защиты обучающихся от угроз сети Интернет.
- Организационная деятельность педагога по обеспечению информационной безопасности обучающихся в сети Интернет.

Тема "Информационная безопасность в сети Интернет" предполагает следующее содержание:

Понятие "информационная безопасность". Составляющие информационной безопасности обучающегося в сети Интернет. Понятие "защита информации". Принципы построения личной системы информационной безопасности в сети Интернет.

Тема "Государственное регулирование в сфере обеспечения информационной безопасности обучающихся при доступе к сети Интернет" ориентирована на следующее содержание:

Законы и иные нормативные акты, регламентирующие обеспечение информационной безопасности обучающихся в сети Интернет. Персональные данные обучающихся. Содержание отдельных статей ФЗ № 152 "О персональных данных", ФЗ № 149 "Об информации, информационных технологиях и защите информации", № 436-ФЗ "О защите детей от информации, причиняющей вред их здоровью и развитию", Концепции информационной безопасности детей, утвержденной распоряжением Правительства Российской Федерации от 2 декабря 2015 г. № 2471-р., Письма Минобрнауки России от 14.05.2018 г. № 08-1184 "О направлении информации" (вместе с "Методическими рекомендациями о размещении на информационных стендах, официальных интернет-сайтах и других информационных ресурсах общеобразовательных организаций и органов, осуществляющих управление в сфере образования, информации о безопасном поведении и использовании сети "Интернет").

Тема "Угрозы информационной безопасности в сети Интернет" предполагает освещение следующих вопросов:

Понятие "угроза информационной безопасности". Классификация угроз. Наиболее распространенные угрозы. Методика определения актуальных угроз информационной безопасности в сети Интернет. Утечка персональных данных. Утечка переписки, личных фотографий (фишинг). Искажение информации. Интернет-зависимость. Кибербуллинг. Угрозы компьютерной технике и программному обеспечению. Кибертерроризм. Киберэкстремизм. Мобильный телефон и угрозы информационной безопасности. Угрозы при работе в общедоступных сетях Wi-fi.

Тема "Меры защиты обучающихся от угроз сети Интернет" предполагает следующее содержание:

Методы защиты от вредоносных программ. Меры обеспечения информационной безопасности при работе в общедоступных сетях Wi-fi. Способы организации безопасной работы обучающихся в социальной сети. Организация безопасной работы с электронной почтой. Методы борьбы с кибербуллингом. Меры по обеспечению безопасности мобильного телефона. Методы предупреждения фишинга (кражи личных данных). Правила проектирования цифровой репутации. Защита авторского права. Этические нормы при работе в сети Интернет. Комплекс мер по защите обучающихся от кибертерроризма, киберэкстремизма. Способы преодоления интернет-зависимости.

Функция “Родительский контроль” при обеспечению информационной безопасности детей в сети Интернет.

Тема “Организационная деятельность педагога по обеспечению информационной безопасности обучающихся в сети Интернет” ориентирована на следующее содержание:

Планирование работы по профилактике безопасного поведения обучающихся в сети Интернет. Рекомендации по планированию и проведению недели “Безопасный Интернет”. Рекомендации по проведению урока безопасности в сети Интернет. Рекомендации по планированию содержания программы внеурочной деятельности по формированию цифровой грамотности обучающихся. Рекомендации по планированию и проведению классных часов по темам:

- Угрозы личной безопасности в сети Интернет.
- Мой профиль в сети Интернет.
- Цифровой след или “Я в сети”.
- Приватность и личные границы. Безопасность в социальной сети.
- Мобильное устройство и безопасность в сети Интернет.
- Безопасное общение в сети Интернет. Сетевой этикет.
- Как построить личную безопасность в сети Интернет и т. п.

Рекомендации по использованию Интернет-ресурсов при планировании и проведении мероприятий по профилактике безопасного поведения обучающихся в сети Интернет.

Организация просветительской работы с родителями (законными представителями) обучающихся. Рекомендации по планированию родительских собраний по темам:

- Безопасность ребенка в сети Интернет. Основные угрозы и как с ними бороться.
- Интернет-зависимость. Как определить и как бороться?
- Мобильное устройство и безопасность в сети Интернет.
- Кибербуллинг. Как помочь ребенку?
- Кибертерроризм и киберэкстремизм. Как защитить себя и ребенка?
- Использование функции “Родительский контроль” при обеспечению информационной безопасности ребенка в сети Интернет.

Рекомендации по использованию Интернет-ресурсов при планировании и проведении просветительской работы с родителями (законными представителями) обучающихся.

3. Рекомендации по актуализации (проектированию) содержания программ повышения квалификации руководящих работников образовательных организаций.

При актуализации (проектировании) содержания программ повышения квалификации руководящих работников образовательных организаций по вопросам обеспечения безопасного пребывания обучающихся в сети Интернет в их содержание могут быть включены следующие темы:

- Информационная безопасность в сети Интернет.
- Государственное регулирование в сфере обеспечения информационной безопасности обучающихся при доступе к сети Интернет.
- Угрозы информационной безопасности в сети Интернет.
- Обеспечение безопасности обучающихся при доступе к сети Интернет.
- Организация работы по обеспечению информационной безопасности обучающихся в образовательной организации.

Тема “Информационная безопасность в сети Интернет” предполагает следующее содержание:

Понятие “информационная безопасность”. Составляющие информационной безопасности обучающегося в сети Интернет. Понятие “защита информации”. Принципы построения системы информационной безопасности обучающихся в сети Интернет. Этапы построения системы информационной безопасности в

образовательной организации. Принципы управления системой информационной безопасности в образовательной организации.

Тема “Государственное регулирование в сфере обеспечения информационной безопасности обучающихся при доступе к сети Интернет” предполагает следующее содержание:

Законы и иные нормативные акты, регламентирующие обеспечение информационной безопасности обучающихся в сети Интернет. Содержание отдельных статей ФЗ № 152 “О персональных данных”, ФЗ № 149 “Об информации, информационных технологиях и защите информации”, № 436-ФЗ “О защите детей от информации, причиняющей вред их здоровью и развитию”, Концепции информационной безопасности детей, утвержденной распоряжением Правительства Российской Федерации от 2 декабря 2015 г. № 2471-р., Письма Минобрнауки России от 14.05.2018 г. № 08-1184 “О направлении информации” (вместе с “Методическими рекомендациями о размещении на информационных стендах, официальных интернет-сайтах и других информационных ресурсах общеобразовательных организаций и органов, осуществляющих управление в сфере образования, информации о безопасном поведении и использовании сети “Интернет”). Локальные акты образовательной организации, регламентирующие безопасный доступ обучающихся к ресурсам сети Интернет.

Тема “Угрозы информационной безопасности в сети Интернет” предполагает следующее содержание:

Понятие “угроза информационной безопасности”. Классификация угроз информационной безопасности обучающихся в сети Интернет. Наиболее распространенные угрозы. Угрозы конфиденциальности. Модели угроз. Методика определения актуальных угроз информационной безопасности обучающихся в сети Интернет. Базовая модель угроз безопасности обучающихся в сети Интернет. Проектирование модели угроз информационной безопасности обучающихся в сети Интернет.

Тема “Обеспечение безопасности обучающихся при доступе к сети Интернет” ориентирована на следующее содержание:

Принципы функционирования компьютерных сетей. Протоколы и технологии сетевого взаимодействия. Варианты организации системы контентной фильтрации в образовательной организации. Меры защиты от вредоносных программ. Методы организации безопасного доступа обучающихся к ресурсам сети Wi-fi. Методы организации безопасной работы обучающихся в социальной сети. Методы организации безопасной работы обучающихся с электронной почтой. Методы предупреждения фишинга (кражи личных данных). Комплекс мер по защите обучающихся от кибертерроризма, киберэкстремизма.

Тема “Организация работы по обеспечению информационной безопасности обучающихся в образовательной организации” предполагает следующее содержание:

Принципы планирования работы по обеспечению информационной безопасности обучающихся в образовательной организации. Алгоритм организации работы по обеспечению информационной безопасности обучающихся при доступе к ресурсам сети Интернет. Состав организационно-распорядительной документации образовательной организации. Организация работы с коллективом в при реализации мер по обеспечению информационной безопасности обучающихся при пребывании в сети Интернет. Подготовка политики образовательной организации в области обеспечения информационной безопасности обучающихся в сети Интернет. Подготовка проектов приказов, локальных актов, инструкций, памяток (для обучающихся, родителей, педагогов) по обеспечению безопасного пребывания обучающихся в сети Интернет. Рекомендации по использованию портала “Сетевичок” и других Интернет-ресурсов при планировании работы по обеспечению информационной безопасности обучающихся в образовательной организации. Проектирование плана работы образовательной организации по обеспечению информационной безопасности обучающихся в сети Интернет.

4. Рекомендации по выбору форм и технологий организации образовательной деятельности слушателей.

Основными формами организации образовательной деятельности слушателей при освоении содержания программ повышения квалификации могут быть:

- лекции;
- практикумы;
- методические тренинги;
- самостоятельное изучение материалов по основным темам курса с использованием электронных образовательных ресурсов;
- просмотр видеолекций;
- вебинары;
- дискуссии;
- круглые столы.

Целесообразно предусмотреть дистанционную поддержку освоения программы повышения квалификации, направленную на предварительную работу слушателей с заранее подготовленными материалами, последующее обсуждение которых может осуществляться в формате вебинара, дискуссии, тренинга, практикума, выстраивая процесс обучения в контексте одной из стратегий смешанного обучения - “перевернутый класс”.

При проведении занятий наряду с использованием технологий формального обучения (технологий коллективного обучения, развития критического мышления и т.п.) рекомендуется использовать технологии неформального обучения.

Неформальное обучение - это любой организованный и устойчивый процесс коммуникации, порождающий обучение, в котором четко обозначены цели, методы, результаты образовательной деятельности и осуществляемый вне рамок системы традиционного обучения.

Основной признак неформального обучения – отсутствие единых, в той или иной мере стандартизированных требований к результатам учебной деятельности слушателей программы повышения квалификации.

Одной из технологий организации неформального обучения является кейс-технология.

Кейс - это учебная конкретная ситуация специально разрабатываемая на основе фактического материала с целью последующего разбора на учебных занятиях.

При использовании этой технологии акцент обучения переносится не на овладение готовым знанием, а на его выработку. Результатом применения кейс-обучения являются не только знания, но и навыки профессиональной деятельности.

Кейс может состоять из нескольких предложений или множества страниц, содержать описание одного события или историю развития нескольких событий на протяжении нескольких лет, представляться в печатном или электронном виде, иметь в содержании:

- текстовые материалы: интервью, фрагмент программы развития, характеристику результатов исследования, статьи и художественные тексты (или их фрагменты), результаты проведенных мониторингов и т. п.;
- иллюстративные материалы: фотографии, диаграммы, таблицы, фильмы, аудиозаписи.

В работе с кейсом выделяют несколько этапов: анализ кейса, групповую дискуссию, моделирование конкретных действий на базе выработанного решения, подведения итогов.

Кейсы целесообразно использовать в работе с педагогами, заместителями руководителей, руководителями образовательных организаций при организации тренингов по решению разного рода педагогических, организационных проблем, для обеспечения дистанционного сопровождения реализации программы повышения квалификации.

Примеры кейсов для организации методических тренингов:
Кейс № 1. Ученица 5 класса рассказала своему классному руководителю, что группа ее одноклассников снимает на фото и видео все, что происходит на перемене. Чтобы было, что снимать, они берут чей-нибудь рюкзак, оставленный в коридоре, выбрасывают его в урну для мусора и ждут, когда владелец рюкзака начнет его искать. Фото и видео ученики выкладывают в разные социальные сети.

Кейс № 2. Заместитель директора по учебно-воспитательной работе получает обращение от родительского комитета одного из классов. 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. Родители просят принять меры. Заместитель директора понимает, что фото с оценками обучающихся сделано с экрана компьютера учителя.

Кейс № 3. К психологу школы за советом обратился ученик 8 класса. Ученик рассказал, что около двух недель назад по электронной почте он получил приглашение от своего друга поиграть в Интернет-игру, доступ к которой открывается по прикрепленной ссылке. Перейдя по указанной в письме ссылке, ученик в появившемся 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 100000 рублей. Родителям рассказать боится. Что предпринять не знает.

Кейс № 4. После первой четверти к директору школы обратилась мама новенькой девочки из 10 класса. Мама сообщила, что в социальной сети появилась группа под названием “Ненавижу новенькую”, к которой присоединилось 60% класса. В группе публикуются сведения, порочащие девочку. На телефон ребенку приходят sms с угрозами и требованиями покинуть класс. Ребенок уходить из класса и из школы не хочет, однако эмоциональное состояние ребенка беспокоит маму. Разговор с классным руководителям не привел к положительному результату.

5. Рекомендации по разработке программ внеурочной деятельности для обучающихся основной и средней школы

При разработке содержания программ внеурочной деятельности “Проектирование личного безопасного цифрового пространства в сети Интернет” для обучающихся основной и средней школы по вопросам безопасного пребывания в сети Интернет в их содержание могут быть включены следующие темы:

- Личное цифровое пространство и его безопасность.
- Электронная почта как основа личного цифрового пространства. Безопасность персональной переписки.
- Облачное хранилище и безопасность личного цифрового пространства.
- Блог и безопасность личного цифрового пространства в сети Интернет.
- Безопасность личного цифрового пространства в социальной сети.
- Информационная безопасность и личный видеоканал в сети Интернет.
- Информационная безопасность и управление личным цифровым пространством с использованием мобильного устройства.
- Презентация личного цифрового пространства в сети Интернет.

Тема “Личное цифровое пространство и его безопасность” предполагает следующее содержание:
Определения понятий “Цифровое пространство”, “Личной цифровое пространство”, “Цифровой след”, “Цифровая репутация”. Основные компоненты личного цифрового

пространства в сети Интернет. Понятие “безопасность личного цифрового пространства”. Актуальные угрозы личного цифрового пространства в сети Интернет.

Тема “Электронная почта, как основа личного цифрового пространства. Безопасность персональной переписки” предполагает следующее содержание:

Электронная почта. Создание электронной почты. Настройка личного электронного ящика (настройка безопасности, оформления, настройка электронной подписи). Электронное письмо. Правила подготовки электронного письма. Работа с входящими письмами (сортировка писем, работа с помеченными письмами, удаление спама, очистка корзины). Актуальные угрозы информационной безопасности при работе с электронной почтой (утечка переписки, взлом личного почтового ящика, спам-рассылка, вирусы и фишинговые ссылки в письме). Методы защиты электронной почты.

Тема “Облачное хранилище и безопасность личного цифрового пространства в сети Интернет” предполагает следующее содержание:

Понятие “Облачное хранилище”. Облачное хранилище, как часть личного цифрового пространства. Виды облачных хранилищ. Основные параметры и характеристики. Возможности облачных хранилищ. Создание папок в облачном хранилище. Загрузка и выгрузка файлов. Создание документа в облачном хранилище. Понятие «совместный доступ». Доступ по адресу. Доступ по ссылке. Совместная работа с документом в облачном хранилище. Создание таблиц. Работа с таблицами в совместном доступе. Создание презентаций. Работа с презентациями в совместном доступе. Выгрузка файлов, созданных в облачном хранилище. Актуальные угрозы информационной безопасности при работе с облачным хранилищем. Организация безопасной работы с облачным пространством в сети Интернет.

Тема “Блог и безопасность личного цифрового пространства в сети Интернет” предполагает следующее содержание:

Определение понятия “Блог”. Блог, как компонент личного цифрового пространства в сети Интернет. Правила создания и ведения блога. Сервисы для создания блога. Разработка структуры личного блога. Дизайн блога. Создание личного блога. Блог и цифровая репутация. Правила проектирования цифровой репутации. Публикация материалов в личном блоге и защита авторского права. Этические нормы при разработке блога.

Тема “Безопасность личного цифрового пространства в социальной сети” предполагает следующее содержание:

Социальная сеть. Виды социальных сетей. Создание групп в социальной сети. Публикация материалов в группе в социальной сети. Сообщества. Создание сообщества. Публикация материалов в сообществе. Группы и форумы. Комментирование в форумах, группах, сообществах. Этические нормы при работе в социальной сети. Социальная сети и цифровая репутация. Правила проектирования цифровой репутации в социальной сети. Актуальные угрозы безопасности личного цифрового пространства в социальной сети. Искажение информации. Кибербуллинг. Способы организации безопасной работы в социальной сети.

Тема “Информационная безопасность и личный видеоканал в сети Интернет” предполагает следующее содержание:

Видеоканал. Правила ведения видеоканала. Правила создания видеоматериалов для личного канала. Личный видеоканал и формирование цифрового имиджа. Создание видеоканала в youtube. Личный видеоканал и информафрмационня безопасность. Личный видеоканал и цифровая репутация. Этические нормы и правила при ведении личного видеоканала.

Тема “Информационная безопасность и управление личным цифровым пространством с использованием мобильного устройства” предполагает следующее содержание:

Работа с электронной почтой с использованием мобильного устройства. Настройка работы с облачным хранилищем на мобильном устройстве. Управление мобильными приложениями (электронные календари, планеры, мессенджеры, загрузки торрентов и

файлов и др). Управление документами на мобильном устройстве. Управление сообществом в социальной сети с использованием мобильного устройства. Мобильный телефон и угрозы безопасности личного цифрового пространства в сети Интернет. Методы защиты от вредоносных программ. Меры обеспечения безопасности при работе в общедоступных сетях Wi-fi. Меры по обеспечению безопасности мобильного телефона.

Тема "Презентация личного цифрового пространства в сети Интернет" предполагает следующее содержание:
Подготовка к презентации личного цифрового пространства в сети Интернет. Презентация личного цифрового пространства в сети Интернет.

При разработке содержания программы внеурочной деятельности следует учесть, что оно должно быть направлено не только на ознакомление обучающихся с актуальными угрозами личного цифрового пространства в сети Интернет, мерами обеспечения безопасности этого пространства, но и на развитие компетенций обучающихся в направлении проектирования безопасного личного цифрового пространства в сети Интернет и его дальнейшего развития.

Основным методом обучения должен стать метод проектов. В этом случае по завершению освоения программы внеурочной деятельности каждый обучающийся сможет представить проект личного безопасного цифрового пространства в сети Интернет или его элемента (блога, сообщества, видеоканала в сети Интернет и т. п).

При реализации метода проектов может быть организована групповая (командная) работа по проектированию безопасного цифрового пространства в сети Интернет. В этом случае по завершению освоения программы внеурочной деятельности группа обучающихся презентует Интернет-проект элемента цифрового пространства (например, сообщество класса, блог класса, облачное пространство класса и т.п.).

Содержание программы внеурочной деятельности рассчитано на обучающихся 6-11 класса. В 6-9 классах в зависимости от уровня сформированности ИКТ-компетентности обучающихся программа внеурочной деятельности может быть реализована в объеме 34 часа (1 час в неделю) или в объеме 68 часов (2 часа в неделю). В 10-11 классах программа внеурочной деятельности может быть реализована в объеме 34 часа в год (1 час в неделю).

При проектировании содержания программы внеурочной деятельности следует учесть, что она может быть реализована модульно в рамках нескольких лет обучения, при этом желательно использовать концентрический подход[1].

[1]Концентрический подход – один из трех основных подходов к построению образовательных программ. Он предполагает периодическое возвращение обучающихся к одному и тому же учебному материалу для все более детального и глубокого его освоения.

Приложение № 1 к методическим рекомендациям по актуализации (проектированию) содержания программ повышения квалификации педагогических и руководящих работников образовательных организаций по вопросам организации информационной безопасности обучающихся при работе в сети Интернет

Ресурсы сети Интернет для использования в работе по обеспечению безопасного пребывания обучающихся в сети Интернет

Название ресурса	Адрес в сети Интернет	Краткая аннотация	Рекомендации по использованию
Единый урок безопасности в сети Интернет	единыйурок.рф	Портал Единыйурок.рф - онлайн-площадка для проведения Единых уроков, тематических занятий и образовательных мероприятий, рекомендованных МОиН РФ. В данном разделе даны методические рекомендации для проведения Единого урока по безопасности в сети Интернет, рекомендации о размещении материалов по этой теме на информационных стендах, официальных интернет-сайтах и других информационных ресурсах общеобразовательных организаций.	Портал может использоваться при проектировании содержания программ повышения квалификации, при проведении методических тренингов, практикумов. Педагогические работники образовательных организаций найдут на сайте рекомендации по проведению единого урока безопасности в сети Интернет, разработке программ внеурочной деятельности по данной теме, станут участниками “Конференции по формированию цифрового детского пространства”, могут пройти дистанционные курсы повышения квалификации “Основы кибербезопасности”, “Информационная компетентность педагога”. Руководящие работники образовательных

			организаций могут использовать материалы портала при планировании мероприятий общешкольного характера, при оформлении информационных стендов, при проведении родительских собраний, обучающих семинаров для педагогов.
Единый урок. Викторины и конкурсы	http://единыйурок.онлайн	В данном разделе портала Единыйурок.рф содержатся тесты, викторины и конкурсы по вопросам обеспечения информационной безопасности детей и молодежи в сети Интернет.	Размещенные тесты, викторины, конкурсы могут использоваться педагогами при проведении занятий внеурочной деятельности, классных часов, единых уроков, посвященных вопросам безопасного пребывания детей в сети Интернет. Мероприятия календаря информационного ресурса могут быть использованы руководящими и педагогическими работниками ОО при планировании работы по обеспечению безопасного пребывания детей в сети Интернет.
Официальный портал МВД России “Безопасный Интернет-детям”	https://xn--b1aew.xn--p1ai/Internet_for_kids	Раздел официального сайта МВД России содержит памятки по обеспечению информационной безопасности детей и молодежи в сети Интернет, тесты на знание правил	Информационный ресурс может использоваться при планировании содержания практикумов в рамках реализации программ повышения квалификации. Материалы будут полезны педагогам при

		поведения в сети Интернет.	организации единых уроков безопасности в сети Интернет, проведении классных часов, оформлении информационных стендов, проведении тематических родительских собраний.
Правила Интернет-безопасности и Интернет-этики для детей и подростков	https://www.gov.spb.ru/gov/terr/reg_kurort/policiya-kurortnogo-rajona/pravila-internet-bezopasnosti-i-internet-etiki-dlya-detej-i-podrostkov/	Раздел официального сайта Администрации Санкт-Петербурга содержит правила Интернет-безопасности и Интернет-этики для детей и взрослых.	Информационный ресурс может использоваться при планировании содержания практикумов в рамках реализации программ повышения квалификации. Материалы будут полезны педагогам при организации единых уроков безопасности в сети Интернет, проведении классных часов, оформлении информационных стендов, проведении тематических родительских собраний.
Центр безопасного Интернета в России	http://www.saferunet.ru/	Центр безопасного Интернета в России является уполномоченным российским членом Европейской сети Центров безопасного Интернета (Insafe). На портале размещена информация для детей и взрослых о различных типах интернет-рисков (опасные программы, интернет-мошенники, кибернижение и др.) и рекомендации	Материалы, размещенные на страницах информационного ресурса может быть рекомендован педагогам образовательных организаций для проектирования содержания программ внеурочной деятельности, уроков безопасности в сети Интернет, классных часов, занятий внеурочной деятельности, тематических родительских собраний.

		по их предотвращению.	Сайт может быть рекомендован обучающимся и родителям (законным представителям) как источник информации об угрозах сети Интернет.
Безопасный Интернет для детей: законодательство, советы, международный опыт	http://i-deti.org/	Информационный ресурс Российской ассоциации электронных коммуникаций содержит нормативно-правовые акты, мнения экспертов, международный опыт по организации просветительской работы в направлении обеспечения информационной безопасности обучающихся. Представлены обучающие и развивающие видеоматериалы, даны ссылки на надежные и безопасные интернет-ресурсы для детей развлекательного и образовательного характера. Видеоролики в простой и доступной форме информируют о всевозможных аспектах взаимодействия пользователей сети Интернет между собой, о неоднозначных и затруднительных ситуациях, которые могут возникнуть во	Информационный ресурс может использоваться при проектировании или актуализации содержания программ повышения квалификации, проведении лекций, методических практикумов. Материалы могут быть использованы руководящими работниками образовательных организаций при планировании работы по обеспечению информационной безопасности обучающихся в образовательной организации. Педагоги могут использовать обучающие и развивающие материалы ресурса при проведении единых уроков безопасности, в работе с родителями, при планировании содержания занятий внеурочной деятельности, классных часов. Ресурс можно рекомендовать детям как источник безопасного контента развлекательного и образовательного характера.

		время пребывания в виртуальном пространстве, о том, как можно решить те или иные проблемы и куда можно обратиться в случае столкновения с недоброжелательностью и нарушением законов об информационной безопасности.	
Портал “Сетевичок”	http://сетевичок.рф	Информационный портал для обеспечения информационной поддержки международного квеста по цифровой грамотности #СЕТЕВИЧОК, конкурса детских и молодежных сайтов #ПРЕМИЯСЕТЕВИЧОК	Информационный ресурс может быть рекомендован педагогами обучающимся при проведении уроков безопасности в сети Интернет. Материалы, представленные на портале, могут использоваться учителями информатики при проведении уроков информатики или занятий внеурочной деятельности, посвященных сайтостроению. Конкурс #ПРЕМИЯСЕТЕВИЧОК будет уместно рекомендовать обучающимся как источник информации по обеспечению безопасности персонального сайта.
Защита детей от вредной информации в сети интернет (Сайт для умных родителей)	http://www.internet-kontrol.ru/	Информационный ресурс для родителей. Собрана подборка статей из о защите детей в Интернете, рассказывается о всевозможных	Подборку статей, размещенных на информационном портале может быть рекомендована родителям (законным представителям) обучающихся в

		поисковых сервисах, созданных специально для детей, о том, как обеспечить защиту детей с помощью настроек операционной системы, какие бывают программы для защиты детей в Интернет.	качестве источника информации об угрозах сети Интернет, способах защиты от угроз сети Интернет. Материалы о поисковых сервисах, созданных специально для детей, о способах обеспечения собственной безопасности в сети с помощью настроек операционной системы могут быть рекомендованы педагогами обучающимся.
Родительский контроль на iOS и Android	https://www.iguides.ru/main/apps/roditelskiy_kontrol_na_ios_i_android_totalnaya_slezhka_za_rebenkom/	На сайте iGuides.ru (медиа о гаджетах, технологиях и играх) размещены рекомендации по обеспечению родительского контроля на iOS и Android при доступе детей к ресурсам сети Интернет.	Информационный ресурс может быть рекомендован родителям при проведении тематических родительских собраний, посвященных вопросам безопасности мобильного Интернета для детей. Инструкции, размещенные на сайте, могут быть использованы при планировании содержания лекций и практикумов в рамках реализации программ повышения квалификации по обеспечению информационной безопасности обучающихся в сети Интернет.
Справочник по детской безопасности в Интернете	www.google.ru/familysafety	Информационный портал Google, который работает в более чем 50 странах мира. Содержит информацию об	Информационный ресурс может быть рекомендован родителям (законным представителям) обучающихся в качестве источника

		инструментах безопасности Google (безопасный поиск, безопасный режим просмотра видео на канале YouTube, настройки возрастных фильтров для мобильных приложений и другое), а также рекомендации ведущих российских организаций, занимающихся вопросами детской безопасности.	информации о способах защиты от угроз сети Интернет. Материалы раздела “Репутация” могут использоваться педагогами образовательных организаций при планировании содержания уроков безопасности, занятий внеурочной деятельности, классных часов, уроков информатики при обсуждении вопросов личной безопасности в сети Интернет. Ресурс можно рекомендовать обучающимся как источник информации о проектировании личного цифрового пространства в сети Интернет.
Безопасный Интернет	http://www.targaltinternetis.ee/ru/	Эстонский информационный портал посвящен вопросам обеспечения информационной безопасности детей и молодежи в сети Интернет. Даны рекомендации о поведении на порталах общения, о безопасном использовании смарт-устройств, как избежать виртуального насилия и др. На страницах портала размещены учебно-информационные материалы для учителей и родителей.	Материалы ресурса могут использоваться при проектировании или актуализации содержания программ повышения квалификации, методических тренингов, семинаров, практикумов для педагогических и руководящих работников образовательных организаций. Материалы могут использоваться педагогическими работниками при проведении единых уроков безопасности, классных часов, декад безопасного Интернета, проектировании содержания программ

			внеурочной деятельности, занятий, в работе с родителями обучающихся.
Министерство юстиции РФ. Федеральный список экстремистских материалов	http://minjust.ru/ru/nko/fedspisok/%27%27?field_extremist_content_value/	Раздел официального сайта Министерства юстиций РФ содержит перечень материалов экстремистского характера, запрещенных к использованию.	Материалы портала могут использоваться при проектировании элементов содержания программ повышения квалификации для руководящих работников образовательных организаций, при проведении лекционных занятий, посвященных проблеме организации контентной фильтрации. Ресурс может быть использован руководящими работниками образовательных организаций при организации системы контентной фильтрации.
Реестр запрещенных сайтов	https://antizapret.info/	Информационный ресурс содержит перечень запрещенных в РФ сайтов и ресурсов. Сайт предназначен исключительно для мониторинга Реестра запрещенных сайтов, не является каталогом.	Материалы портала могут использоваться при проектировании элементов содержания программ повышения квалификации для руководящих работников образовательных организаций, при проведении лекционных занятий, посвященных проблеме организации контентной фильтрации. Ресурс может быть использован руководящими работниками образовательных организаций при организации системы

			контентной фильтрации.
CNews Безопасность	http://safe.cnews.ru/news/top/2017-12-12_belye_spiski_v_runete_zarabotayut_vesnoj_2020	Новостной ресурс сети Интернет по вопросам обеспечения информационной безопасности детей и молодежи в сети Интернет	Новостной ресурс будет полезен при проектировании содержания лекционного материала в рамках реализации программ повышения квалификации для педагогических и руководящих работников системы образования. Ресурс может быть рекомендован руководящим работникам образовательных организаций как источник актуальных новостей об изменениях в сфере обеспечения информационной безопасности детей в сети Интернет.
Сайт Лаборатории Касперского “Защита детей”	https://kids.kaspersky.ru/category/articles/ Образовательные мультфильмы “Приключение робота Каспера и мальчика Севы” https://kids.kaspersky.ru/category/entertainment/multfilmy/	Раздел сайта содержит информацию об угрозах сети Интернет, рекомендации по организации защиты детей от угроз сети Интернет. Анимационный материал на примере приключений Каспера и Севы рассказывает о возможных угрозах сети Интернет. Каждый мультипликационный сюжет представляет собой видеоинструкцию по безопасному поведению обучающихся	Материалы, опубликованные на сайте, могут быть использованы при при разработке материалов для проведения лекций, практикумов, тренингов. Педагоги могут использовать содержание сайта при проектировании программ внеурочной деятельности, проведении уроков безопасности в сети Интернет, классных часов, тематических родительских собраний. Анимационный сериал может быть рекомендован учителям начальной школы при

		начальной школы в сети Интернет.	планировании содержания уроков безопасного поведения в сети Интернет. и родителям (законным представителям) обучающихся в рамках тематического родительского собрания.
Азбука цифрового мира.	https://www.edu.yar.ru/azbuka/	На сайте размещены увлекательные комиксы, специализированные тренажёры и интересные игры.	Материалы сайта будут полезны педагогам при проработке содержания программы внеурочной деятельности, уроков безопасности в сети Интернет, классных часов, занятий внеурочной деятельности. Комиксы и тренажеры могут быть рекомендованы обучающимся как общеразвивающий безопасный контент сети Интернет. Методический материал может быть использован при реализации программ повышения квалификации.
Портал детской безопасности “СПАСЭКСТРИМ” МЧС России.	http://www.spas-extreme.ru/themes/internet_bezopasnost	В разделе портала, посвященному Интернет-безопасности, размещены правила безопасной работы в сети Интернет, тесты.	Методические материалы могут использоваться педагогами при оформлении уголков безопасности в сети Интернет, проведении уроков безопасности, классных часов, в работе с родителями (законными представителями) обучающихся.
Персональные данные. Дети.	http://xn--80aalcbc2bocdadlpp9nfk.xn--d1acj3b/	Портал проекта Роскомнадзора “Персональные	Материал знакомит обучающихся 6-11 класса с понятием

		данные. Дети” содержит базу материалов в виде правил, памяток, презентаций, тестов и игр по актуальным вопросам безопасности персональных данных обучающихся в сети Интернет.	персональные данные, правилами конфиденциальности в сети Интернет. Среди представленных материалов размещены инструкции для родителей (законных представителей), педагогов. Представленные материалы могут использоваться педагогами при подготовке к проведению уроков безопасности в сети Интернет, занятий внеурочной деятельности, классных часов.
Электронный журнал для детей “Филипок”	http://www.filipoc.ru/interesting/bezopasnyiy-internet-dlya-detey	Электронный журнал для детей, на страницах которого опубликованы правила безопасного поведения в сети Интернет, занимательные викторины, ребусы и игры по цифровой грамотности.	Электронный журнал может быть рекомендован учителям начальных классов образовательных организаций для проектирования содержания уроков безопасности в сети Интернет, классных часов, занятий внеурочной деятельности.

Приложение № 2 к методическим рекомендациям по актуализации (проектированию) содержания программ повышения квалификации педагогических и руководящих работников образовательных организаций по вопросам организации информационной безопасности обучающихся при работе в сети Интернет

Программное обеспечение и сервисы сети Интернет для организации контентной фильтрации

DNS-фильтры[2]:

Название	Адреса
Яндекс.DNS Семейный dns.yandex.ru	77.88.8.7 77.88.8.3
NetPolice DNS http://old.netpolice.ru/filters/dns-filter/	81.176.72.82 81.176.72.83

Системы контентной фильтрации (СКФ)[3]:

Название, адрес СКФ	Краткая аннотация
SkyDNS для учебных заведений https://www.skydns.ru/	Облачная фильтрация или отдельное устройство на базе беспроводного роутера. Фильтрация осуществляется по принципу dns-фильтрации. Для эффективной работы требуется наличие публичного ip-адреса (статического или динамического).
Контент-фильтр ИКС для школ https://xserver.a-real.ru/editions/resheniya/obrazovanie.php	Решение, созданное на базе свободного программного обеспечения, работает как интернет-шлюз для локальной сети. Функционал расширяется до UTM-решения, поддерживаются антивирусные решения для шлюзов ДрВеб и Лаборатория Касперского, система обнаружения и предотвращения вторжений. Версия до 8 пользователей бесплатна полностью. Имеет контент фильтр, категории трафика SkyDNS. Включен в Единый Реестр Российского ПО для ЭВМ и БД.

[2] Сервисы являются бесплатными и работают по принципу “черных списков”. Не требуют установки и перенастройки сети, обеспечивают минимальный уровень фильтрации, не имеют возможностей по настройке.

[3] Полноценные программные или программно-аппаратные коммерческие решения для установки на компьютеры пользователей и\или сервера в локальной сети. Каждое из решений предполагает наличие пробного периода для оценки удобства и эффективности использования в конкретной образовательной организации.

	Имеет сертификат ФСТЭК.
Персональный клиент фильтрации «NetPolice PRO» для образовательных учреждений. http://www.netpolice.ru/collection/school	Предназначен для защиты отдельных ПК, поддерживает только операционными системами семейства Microsoft Windows, имеет ограничения по работе с браузерами.
Traffic Inspector School Edition http://www.smart-soft.ru/solutions/schools/	Решение является шлюзом безопасности локальной сети, включено в Единый Реестр Российского программного обеспечения (ПО) для ЭВМ и БД. Имеет сертификат ФСТЭК. Осуществляется перехват и расшифровка защищенных соединений HTTPS. Интеграция с Microsoft Active Directory. Предлагается в качестве ПО, устанавливаемого на шлюзовой компьютер под управление ОС Windows 7 и выше, в том числе серверных версий.
UserGate Web Filter http://www.entensys.com/ru/products/usergate-web-filter/overview	Семейство продуктов компании Entensys для защиты локальной сети, где контент-фильтр является одним из модулей комплексной защиты UserGate UTM, который объединяет межсетевой экран нового поколения (Next Generation Firewall), систему обнаружения вторжений, защиту от вредоносных программ и вирусов, систему контент-фильтрации, серверный антиспам, VPN-сервер и другие функции в едином решении. Включен в Единый Реестр Российского ПО для ЭВМ и БД. Имеет сертификат ФСТЭК и как межсетевой экран и как система обнаружения вторжений. Имеет как аппаратное исполнение, так и как виртуальная машина.
Kinder Gate http://www.kindergate-parental-control.com/ru	Продукт компании Entensys, предназначен для защиты отдельных ПК, но возможна установка в кластер для централизованного управления. Поддерживаются операционными системами Windows/Linux/MacOS.

Рекомендации по антивирусной защите:

Лаборатория Касперского (www.kaspersky.ru)	Лабораторией предлагаются варианты решений от полнофункционального бесплатного антивируса (Kaspersky Free) до комплексной системы защиты сети. Включен в Единый Реестр Российского ПО

	для ЭВМ и БД. Имеет сертификаты ФСТЭК. Предлагается как компонент защиты на межсетевых экранах. Занимает лидирующие позиции как в отечественных, так и в иностранных рейтингах. Лидер на рынке СНГ. Входит в четверку мировых разработчиков антивирусных решений.
Доктор Веб (www.drweb.ru)	Варианты решений от бесплатного антивирусного сканера (Dr.Web CureIt) до комплексной системы защиты сети. Включен в Единый Реестр Российского ПО для ЭВМ и БД. Имеет сертификаты ФСТЭК. Компания отказалась от участия в сравнительных тестированиях.
ESET (www.esetnod32.ru)	Существуют варианты решений от бесплатных утилит до комплексной системы защиты сети. Имеет сертификаты ФСТЭК.

Приложение № 3 к методическим рекомендациям по актуализации (проектированию) содержания программ повышения квалификации педагогических и руководящих работников образовательных организаций по вопросам организации информационной безопасности обучающихся при работе в сети Интернет

Рекомендации законодательных и исполнительных органов власти РФ по организации работы по обеспечению безопасного пребывания обучающихся в сети Интернет.

1. Доктрина информационной безопасности РФ (утв. Президентом РФ 09.09.2000 N Пр-1895).

2. Федеральный закон от 29.12.2010 № 436-ФЗ "О защите детей от информации, причиняющей вред их здоровью и развитию".

3. ГОСТ Р 50739-95 Средства вычислительной техники. Защита от несанкционированного доступа к информации. Общие технические требования (принят постановлением Госстандарта РФ от 9 февраля 1995 г. № 49).

4. Распоряжение Правительства Российской Федерации от 02.12.2015 № 2471-р "Об утверждении Концепции информационной безопасности детей".

5. Письмо Минобрнауки России от 28.04.2014 № ДЛ-115/03 "О направлении методических материалов для обеспечения информационной безопасности детей при использовании ресурсов сети Интернет" (вместе с "Методическими рекомендациями по ограничению в образовательных организациях доступа обучающихся к видам информации, распространяемой посредством сети "Интернет", причиняющей вред здоровью и (или) развитию детей, а также не соответствующей задачам образования").

6. Письмо Минобразования РФ от 13.08.2012 № 01-51-088ин "Об организации использования информационных и коммуникационных ресурсов общеобразовательных учреждений".

7. Письма Минобрнауки России от 14.05.2018 г. № 08-1184 "О направлении информации" (вместе с "Методическими рекомендациями о размещении на информационных стендах, официальных интернет-сайтах и других информационных ресурсах общеобразовательных организаций и органов, осуществляющих управление в сфере образования, информации о безопасном поведении и использовании сети "Интернет").

8. Рекомендаций парламентских слушаний "Актуальные вопросы обеспечения безопасности и развития детей в информационном пространстве" от 17 апреля 2017 г.

Приложение № 4 к методическим рекомендациям по актуализации (проектированию) содержания программ повышения квалификации педагогических и руководящих работников образовательных организаций по вопросам организации информационной безопасности обучающихся при работе в сети Интернет

Методические материалы для организации работы по обеспечению безопасного пребывания обучающихся в сети Интернет в образовательных организациях

Название методического материала	**Название сайта/автор**	**Адрес в сети Интернет**	**Рекомендации по использованию**

Методические рекомендации для педагогов “Основы кибербезопасности”	Портал “Единый урок”. Календарь. Методики. Материалы”	https://www.xn--d1abkefqip0a2f.xn--p1ai/index.php/4/152-osnovy-kiberbezopasnosti?showall=&start=3	Методические рекомендации, разработанные членами и экспертами Временной комиссии Совета Федерации по развитию информационного общества, включают в себя межпредметный курс внеурочной деятельности для начального, общего и полного среднего образования “Основы кибербезопасности”. Курс разработан в соответствии с требованиями и целями ФГОС и Стратегии развития отрасли информационных технологий в Российской Федерации. Отдельные тематические блоки курса могут быть внедрены в содержание учебных программ образовательных организаций таких предметов как “Информатика”, “ОБЖ”, “Биология”. Материалы могут использоваться при проектировании содержания программ повышения квалификации для педагогических и руководящих работников образовательных организаций, при проведении практикумов, лекционных занятий.
Курс “Основы кибербезопасности”	Тонких И.М. Комаров М.М. Ледовской В.И. Михайлов А.В., Москва, 2016 г.	https://drive.google.com/file/d/0B3aUlJMM2qjobHJPNGVESFlnZXc/view	Методический материал представляет собой межпредметный курс, посвященный актуальным вопросам обеспечения безопасности в сети

			Интернет (техника безопасности и эргономика, сетевой этикет, мошеннические действия в сети Интернет, правовые основы кибербезопасности и т.д.). Курс построен по модульному принципу. Каждый модуль может использоваться как элемент содержания при разработке программы внеурочной деятельности. Методический материал содержит примеры разработок уроков, посвященных способам защиты от угроз сети Интернет. Представленные материалы будут полезны педагогам при проектировании содержания программ внеурочной деятельности, уроков информационной безопасности. Курс может быть использован в рамках реализации программ повышения квалификации при проведении практикумов и тренингов.
Материалы к урокам безопасного Интернета	Официальный сайт “Лига безопасного Интернета”	http://www.ligainternet.ru/encyclopedia-of-security/parents-and-teachers/parents-and-teachers-detail.php?ID=3652	Методические материалы представляют собой подборку разработанных презентаций к урокам информационной безопасности в сети Интернет. Презентации могут быть использованы педагогами образовательных организаций в рамках уроков безопасности,

			занятий внеурочной деятельности.
Онлайн-курс “Безопасность в Интернете” от Академии Яндекса	Образовательная Интернет-платформа Stepik	https://stepik.org/course/191/	Онлайн-курс содержит информацию о видах мошенничества в сети Интернет и о том, как им противостоять. Курс рассчитан на обучающихся 6—9 классов, но он будет полезен родителям, педагогам, планирующим проведение урока по безопасности в сети Интернет. В курсе три раздела. Каждый раздел состоит из конспекта для самостоятельного изучения, видео-урока и теста, для организации самоконтроля. Материалы курса будут полезны при подготовке лекционного материала, практикумов, обеспечения дистанционной поддержки реализации программ повышения квалификации для педагогических работников. Материалы курса имеют бесплатный доступ.
Методическое пособие “Медиаграмотность. Как жить в медиамире”	Дубовер Д. Донской государственный технический университет, Областной центр медиаграмотности. Ростов-на-Дону, 2015 г.	https://biuv-school9tihvin.eduface.ru/uploads/24300/24236/section/451751/DOT/Metodicheskoe_posobie_Mediagramotnost_.pdf	Методическое пособие на доступном уровне рассказывает о безопасном поведении ребенка в социальной сети, новостной грамотности, о безопасной работе с почтовым сервисом и облачным хранилищем, об использовании электронных денег и организации родительского контроля. Пособие может быть использовано педагогами

			при планировании содержания программы внеурочной деятельности, уроков безопасности, классных часов, тематических родительских собраний. Электронное пособие может быть рекомендовано обучающимся и родителям (законным представителям). Материалы пособия могут использоваться при реализации программ повышения квалификации.
Методическое пособие “ИНТЕРНЕТ: ВОЗМОЖНОСТИ, КОНЦЕПЦИИ, БЕЗОПАСНОСТЬ” Часть 1.	Солдатова Г., Золотова Е., Лебешева М., Шляпников В. Фонд Развития Интернет ФГАУ “Федеральный институт развития образования” Министерства образования и науки РФ Факультет психологии МГУ имени М. В. Ломоносова, 2013 г.	http://s_194.edu54.ru/DswMedia/booktheorye.pdf	Методическое пособие раскрывает аспекты цифрового гражданства личности в сети Интернет, технологические аспекты работы в сети Интернет, об информации в сети Интернет и правилами работы с нею, способах безопасной коммуникации и цифровой коммерции. Пособие может быть использовано педагогами при планировании содержания программы внеурочной деятельности, уроков безопасности, классных часов, тематических родительских собраний. Материалы пособия могут использоваться при реализации программ повышения квалификации.
Методическое пособие “ИНТЕРНЕТ: ВОЗМОЖНОСТИ, КОНЦЕПЦИИ, БЕЗОПАСНОСТЬ” Часть 2 (практикум).	Солдатова Г., Золотова Е., Лебешева М., Шляпников В. Фонд Развития Интернет ФГАУ «Федеральный	http://s_194.edu54.ru/DswMedia/book_praktikum.pdf	Методическое пособие представляет собою подборку разработок уроков информационной безопасности по следующим тематическим блокам:

	институт развития образования» Министерства образования и науки РФ Факультет психологии МГУ имени М. В. Ломоносова, 2013 г.		цифровое гражданство, технологические аспекты работы в сети Интернет, информация в сети Интернет, коммуникации в сети Интернет, цифровое потребление. Пособие может стать основой для проработки содержания программы внеурочной деятельности. Материалы пособия могут использоваться при реализации программ повышения квалификации.
Методическое руководство “Полезный и безопасный Интернет. Правила безопасного использования интернета для детей младшего школьного возраста”	Солдатова Г. У. Федеральный институт развития образования, 2012 г.	http://s_194.edu54.ru/DswMedia/metodika.pdf	Методическая разработка адресована психологам, педагогам начальных классов, классным руководителям, родителям школьников младших классов, представляет собой методическое руководство по планированию занятий с обучающимися начальной школы, посвященных вопросам безопасного пребывания в сети Интернет. Пособие может использоваться педагогами при проработке содержания программы внеурочной деятельности, отдельных занятий и уроков. Руководство может быть рекомендовано родителям (законным представителям) обучающихся в рамках тематического родительского собрания.
Материалы Всероссийского вебинара “Профилактика	Федеральное государственное бюджетное научное	Учебные материалы: http://fcprc.ru/training/webinars/12-17/educational-docs	Учебные материалы представляют собой видеолекции ведущих специалистов в области

суицидального поведения детей и подростков, связанного с влиянием сети Интернет” , декабрь 2017 г.	учреждение “Центр защиты прав и интересов детей”	Методические материалы: http://fcprc.ru/training/webinars/12-17/method-docs	обеспечения детской безопасности в сети Интернет по следующим тематическим направлениям: психолого-педагогические подходы к профилактике рисков и угроз современной Интернет-среды; экспертная деятельность педагогов по оценке интернет-контента и обнаружению информации, причиняющей вред здоровью и развитию обучающихся; защита детей и подростков от информации о способах совершения самоубийства и призывах к совершению самоубийства, размещенной в сети «Интернет». Методические материалы представляют собой рекомендации по организации профилактической работы с обучающимися по вопросам безопасного пребывания в сети Интернет. Учебные и методические материалы одобрены министерством просвещения РФ и могут быть использованы в рамках реализации программ повышения квалификации для руководящих и педагогических работников образовательных организаций, использоваться педагогами при планировании содержания тематических родительских собраний,

			уроков информационной безопасности в сети Интернет.
Учебно-методическое пособие “Практическая психология безопасности: управление персональными данными в Интернете”	Солдатова Г.У., Приезжева А.А., Олькина О.И., Шляпников В.Н. Федеральный институт развития образования. Фонд развития Интернет. Координационный центр национального домена сети Интернет, 2017 г.	http://collegelaw.ru/downloads/file_655.pdf	Учебно-методическое пособие посвящено решению задачи повышения цифровой компетентности обучающихся, педагогов, родителей в сфере управления персональными данными в сети Интернет. В пособии проанализированы теоретические и методические аспекты проблемы приватности и персональных данных в сети Интернет. Учебно-методическое пособие включает в себя разработки уроков для педагогов, практикум для обучающихся 6–10-х классов. Материалы к урокам подготовлены с учетом действующего законодательства РФ, а также мирового опыта управления персональными данными в интернете. Материалы пособия могут быть использованы педагогами при планировании содержания программы внеурочной деятельности по актуальным аспектам обеспечения информационной безопасности в сети Интернет, планировании уроков безопасности, классных часов, тематических родительских собраний. Учебно-методическое пособие можут быть использовано в определении содержания

			программ повышения квалификации для педагогических работников образовательных организаций, подготовке методических тренингов и практикумов.
Дидактическая игра #БУДЬСМЕЛЫМ	Официальный сайт компании Tight on the Internet - Безопасный интернет-центр в Эстонии SIC IV IV	Инструкция: https://suurimjulgus.ee/assets/files/Telia_juhis_RU_315x280.pdf Материалы для организации игры: https://suurimjulgus.ee/assets/files/Telia_kaardid_RUS_A4_print.pdf	Дидактическая игра #БУДЬСМЕЛЫМ представляет собой набор кейсов, связанных с разными угрозами сети Интернет. В каждой ситуации обучающиеся должны синтезировать решения проблемы, с которой столкнулся персонаж кейса. Дидактическая игра может использоваться педагогами при проведении уроков безопасности, занятий внеурочной деятельности, уроков информатики, посвященных безопасности в сети Интернет. Методический материал может быть использован при проведении методических тренингов, практикумов с педагогами в рамках реализации программы повышения квалификации.

Приложение № 5 к методическим рекомендациям по актуализации (проектированию) содержания программ повышения квалификации педагогических и руководящих работников образовательных организаций по вопросам организации информационной безопасности обучающихся при работе в сети Интернет

Учебно-методические материалы для обеспечения реализации программы повышения квалификации для педагогических и руководящих работников образовательных организаций

Название	**Название организации-разработчика**	**Ссылка**	**Краткая аннотация**
Информационная безопасность. Основные понятия и направления работы.	Отдел учебно-методической работы ГБУ ДПО “Санкт-Петербургский центр оценки качества образования и информационных технологий”, 2018 г.	https://drive.google.com/file/d/1CQ0LMVk_awzw6-nE0SnCOtZw5C0Ainhi/view?usp=sharing	Презентация раскрывает суть понятий “информационная безопасность”, “защита информации”, “угроза информационной безопасности”. В презентации сделан акцент на основных направлениях обеспечения информационной безопасности в образовательной организации, принципах построения системы информационной безопасности. Материал может быть использован в рамках реализации программы повышения квалификации для педагогических и руководящих работников образовательных организаций.
Информационная безопасность.	Отдел учебно-методическ	https://drive.google.com/file/d/1pp1G1R	Презентация представляет собой

Требования законодательства РФ	ой работы ГБУ ДПО “Санкт-Петербургский центр оценки качества образования и информационных технологий”, 2018 г.	FqkjKAA_4Al0sQLexH3AqBYvHL/view?usp=sharing	навигатор по основным нормативно-правовым актам РФ, регламентирующим обеспечение информационной безопасности участников образовательных отношений. Материал может быть использован в рамках реализации программы повышения квалификации для руководящих работников образовательных организаций.
Информационная безопасность в ОО. Подготовка ОРД	Отдел учебно-методической работы ГБУ ДПО “Санкт-Петербургский центр оценки качества образования и информационных технологий”, 2018 г.	https://drive.google.com/file/d/1Nx2mBOCxxQouPibU7tt_ETOB2gpmurCN/view?usp=sharing	Презентация акцентирует внимание на нормативно-правовых актах РФ, регламентирующих обеспечение информационной безопасности участников образовательных отношений, которые являются основой для разработки организационно-распорядительной документации образовательной организации. В презентации приведен примерный перечень организационно-распорядительной документации по вопросам обеспечения информационной безопасности участников

			образовательных отношений. Материал может быть использован в рамках реализации программы повышения квалификации для руководящих работников образовательных организаций.
Интернет в ОО. Нормативные акты	Отдел учебно-методической работы ГБУ ДПО “Санкт-Петербургский центр оценки качества образования и информационных технологий”, 2018 г.	https://drive.google.com/file/d/11GAuD1uTF535-zeQ0TppmdiOpBI3EGcl/view?usp=sharing	Презентация представляет собой навигатор по основным нормативно-правовым актам РФ, регламентирующим обеспечение безопасный доступ обучающихся к ресурсам сети Интернет. Материал может быть использован в рамках реализации программы повышения квалификации для руководящих работников образовательных организаций.
Интернет в ОО. Организация контентной фильтрации	Отдел учебно-методической работы ГБУ ДПО “Санкт-Петербургский центр оценки качества образования и информационных технологий”, 2018 г.	https://drive.google.com/file/d/1BuDFkJmepwxyhdha0rugbGTbZdIvknYA/view?usp=sharing	Презентация посвящена вопросам организации контентной фильтрации в образовательной организации. В презентации приводятся варианты построения системы контентной фильтрации для обеспечения безопасного доступа

			обучающихся к ресурсам сети Интернет. Материал может быть использован в рамках реализации программы повышения квалификации для руководящих работников образовательных организаций.
Кейсы для организации методических тренингов по теме “Информационная безопасность в сети Интернет”	Отдел учебно-методической работы ГБУ ДПО “Санкт-Петербургский центр оценки качества образования и информационных технологий”, 2018 г.	http://umr.rcokoit.ru/pages/methodical-cabinet-is-network.html	Кейсы представляют собой несколько сюжетных задач, связанных с конкретной угрозой сети Интернет. Представленные кейсы могут быть использованы при проведении методических тренингов в рамках реализации программ повышения квалификации как для педагогических работников, так и для руководящих работников образовательных организаций.

Методические рекомендации разработаны специалистами
ГБУ ДПО «Санкт-Петербургского центра оценки качества образования и информационных технологий» и предназначены для государственных образовательных учреждений дополнительного профессионального образования, находящихся в ведении Комитета по образованию Санкт-Петербурга.

Авторы - составители:
Дорофеева Татьяна Владимировна, заведующий сектором отдела учебно-методической работы ГБУ ДПО “СПбЦОКОиИТ”.
Туманов Иван Анатольевич, методист отдела учебно-методической работы ГБУ ДПО “СПбЦОКОиИТ”.