**ЧАСТНОЕ ДОШКОЛЬНОЕ ОБРАЗОВАТЕЛЬНОЕ УЧРЕЖДЕНИЕ**

**«ДЕТСКИЙ САД №89 ОТКРЫТОГО АКЦИОНЕРНОГО ОБЩЕСТВА**

**«РОССИЙСКИЕ ЖЕЛЕЗНЫЕ ДОРОГИ»**

**МЕТОДИЧЕСКИЕ РЕКОМЕНДАЦИИ**

**Реализация мероприятий,**

**направленных на профилактику рисков и угроз для детей, связанных с использованием современных информационных технологий информационно-телекоммуникационной**

**сети «Интернет»**

**в образовательных организациях**

**открытого акционерного общества**

**«Российские железные дороги»**



**Автор-составитель:**

**Зам зав по УВР**

**Е.С. Червякова**

**Ярославль 2021 г.**

**Информационная безопасность** – защищенность информации от случайных или преднамеренных воздействий, обеспечение конфиденциальности, целостности и доступности информации.

Согласно законодательству Российской Федерации, информационная безопасность детей – 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 (Федеральный закон от29.12.2010 № 436-ФЗ «О защите детей от информации, причиняющей вред их здоровью и развитию»).

Данные методические рекомендации опираются на Письмо Минпросвещения России от 29 марта 2019 года № 03-393 и являются методическими рекомендациями по реализации мер, направленных на обеспечение безопасности несовершеннолетних в сети «Интернет», (далее – Рекомендации) разработаны на основе положений:

1. Федерального закона от 29.12.2010 № 436-ФЗ «О защите детей от информации, причиняющей вред их здоровью и развитию»;

2. Федерального закона от 27.07.2006 г. № 149-ФЗ «Об информации, информационных технологиях и о защите информации»

3. Федеральный закон от 02.07.2013 г. № 187-ФЗ «О внесении изменений в отдельные законодательные акты Российской Федерации по вопросам защиты интеллектуальных прав в информационно-телекоммуникационных сетях

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

5. Рекомендаций парламентских слушаний «Актуальные вопросы обеспечения безопасности и развития детей в информационном пространстве», прошедших в Совете Федерации 17 апреля 2017 года;

6. Международной практики деятельности государственных органов по обеспечению защиты детей от информации, причиняющей вред их здоровью и развитию, и саморегулированию в сети «Интернет».

Рекомендации направлены на расширение в образовательных учреждениях открытого акционерного общества «Российские железные дороги» (далее ОАО «РЖД») внедрения механизмов обеспечения информационной защиты несовершеннолетних пользователей организациями и физическими лицами, осуществляющими деятельность в информационно-телекоммуникационной сети «Интернет» (далее – образовательные организации и физические лица), посредством разработки и администрирования Интернет-ресурсов, сервисов и других технических программных решений.

Рекомендации носят рекомендательный характер и содержат:

1. Принципы организации зашиты несовершеннолетних пользователей, рекомендованные к руководству в повседневной работе организаций и физических лиц;

2. Меры по организации защиты несовершеннолетних пользователей в сети «Интернет», включающие необходимые организационные мероприятия, перечень функций и опции сайтов и сервисов для детей и родителей (законных представителей).

3. Примерные направления работы образовательных организаций ОАО «РЖД» **направленных на профилактику рисков и угроз для детей, связанных с использованием современных информационных технологий информационно-телекоммуникационной сети «Интернет».**

4. Приложения (1-4).

5. Приложение 5. Примерный план мероприятий по обеспечению информационной безопасности и безопасному использованию сети «Интернет» в образовательных организациях ОАО «РЖД».

**Принципы обеспечения реализации комплекса мер, направленных на обеспечение безопасности несовершеннолетних в сети «Интернет»**

При реализации комплекса административных и организационных мер, направленных на обеспечение безопасности детей в сети «Интернет», образовательным организациям и физическим лицам рекомендуется учитывать международную практику обеспечения информационной безопасности несовершеннолетних:

1. Статьи 13, 17, 34 «Конвенции о правах ребенка» Генеральной Ассамблеи ООН обязывают государства-участников обеспечивать разработку «надлежащих принципов защиты ребенка от информации и материалов, наносящих вред его благополучию», а также устанавливать необходимые ограничения прав самого ребенка, включая «свободу искать, получать, передавать информацию и идеи любого рода». Статья 19 Конвенции закрепляет обязанность государств принимать «все необходимые законодательные, административные, социальные и просветительные меры с целью защиты ребенка от всех форм физического или психологического насилия, оскорбления или злоупотребления, отсутствия заботы или небрежного обращения, грубого обращения или эксплуатации, включая сексуальное злоупотребление, со стороны родителей, законных опекунов или любого другого лица, заботящегося о ребенке»;

2. Статья 20 «Международного пакта о гражданских и политических правах» от 16 декабря 1966 г. предусматривает, что «всякая пропаганда войны», а также «всякое выступление в пользу национальной, расовой или религиозной ненависти, представляющее собой подстрекательство к дискриминации, вражде или насилию, должно быть запрещено законом»;

3. Пункт 5 Статьи 9 Палермского Протокола от 15 ноября 2000 года предусматривает введение запрета на производство и оборот материалов, пропагандирующих преступления, связанные с торговлей людьми, включая пропаганду порнографии, эксплуатации проституции и иных коммерческих сексуальных услуг;

4. Статья 15 Модельного закона «Об основных гарантиях прав ребенка в государстве» № 14-9, принятого постановлением на четырнадцатом пленарном заседании Межпарламентской Ассамблеи государств-участников СНГ от 16 октября 1999 г., устанавливает основные гарантии защиты ребенка от информации, пропаганды и агитации, наносящих вред его здоровью, нравственному и духовному развитию. Закон обязывает органы государственной власти принимать меры по защите ребенка от информации, пропаганды и агитации, наносящих вред его здоровью, нравственному и духовному развитию, в том числе, от национальной, классовой, социальной нетерпимости, от рекламы алкогольной продукции и табачных изделий, от пропаганды социального, расового, национального и религиозного неравенства, а также от распространения печатной продукции, аудио- и видеопродукции, пропагандирующей насилие и жестокость, порнографию, наркоманию, токсикоманию, антиобщественное поведение.

*Примечание:*

*Важно отметить, что Европейский суд по правам человека признал защиту нравственности в демократическом обществе легитимной целью ограничения свободы выражения мнения, в соответствии с частью 2 статьи 10 «Европейской конвенции по правам человека». Суд подтвердил, что государства вправе принимать законы, ограничивающие распространение информации и идей, несмотря на их достоинства «как произведений искусства или как вклада в публичное обсуждение проблем», в том числе устанавливать контроль и классификацию информационной продукции. При нарушении закона предусмотрено применение штрафных мер, конфискации и других санкций, вплоть до уголовных, когда это необходимо в интересах защиты нравственности и благополучия конкретных лиц или групп лиц /таких как дети), нуждающихся в особой охране, в связи с недостатком зрелости или состоянием зависимости.*

К правовым основам информационной безопасности детей на территории Российской Федерации можно отнести:

1. Федеральный закон от 29 декабря 2010 г. № 436-ФЗ «О защите детей от информации, причиняющей вред их здоровью и развитию», регулирующий отношения, связанные с защитой детей от информации, причиняющей вред их здоровью и (или) развитию, в том числе от такой информации, содержащейся в информационной продукции;

2. Федеральный закон от 3 июля 1998 г. № 124-ФЗ «Об основных гарантиях прав ребенка в Российской Федерации», устанавливающий обязанность органов государственной власти Российской Федерации принимать меры по защите ребенка от информации, пропаганды и агитации, наносящих вред его здоровью, нравственному и духовному развитию, в том числе от национальной, классовой, социальной нетерпимости, от рекламы алкогольной продукции и табачных изделий, от пропаганды социального, расового, национального и религиозного неравенства, от информации порнографического характера, от информации, пропагандирующей нетрадиционные сексуальные отношения, а также от распространения печатной продукции, аудио- и видеопродукции, пропагандирующей насилие и жестокость, наркоманию, токсикоманию, антиобщественное поведение.

В соответствии с приказом Минкомсвязи России от 16.06.2014 № 161 «Об утверждении требований к административным и организационным мерам, техническим и программно-аппаратным средствам защиты детей от информации, причиняющей вред их здоровью и (или) развитию», требования к административным и организационным мерам, техническим и программно-аппаратным средствам защиты детей от информации, причиняющей вред их здоровью и (или) развитию, применяются при обороте информационной продукции, содержащей информацию, запрещенную для распространения среди детей, в соответствии с частью 2 статьи 5 Федерального закона от 29 декабря 2010 г. № 436-Ф3 «О защите детей от информации, причиняющей вред их здоровью и развитию», в местах, доступных для детей, а также при предоставлении, в соответствии с частью 1 статьи 14 Федерального закона № 436-Ф3 доступа к информации, распространяемой посредством информационно-телекоммуникационных сетей, в том числе сети «Интернет», в местах, доступных для детей.

При этом, в целях обеспечения информационной безопасности детей, организациям и физическим лицам рекомендуется реализовать комплекс административных и организационных мер, технических и программно-аппаратных средств защиты детей от информации, причиняющей вред их здоровью и (или) развитию.

**Общие положения**

**Методических рекомендаций о реализации мер, направленных на обеспечение безопасности несовершеннолетних**

**в сети «Интернет»**

Образовательным организациям и физическим лицам, осуществляющим деятельность в информационно-телекоммуникационной сети «Интернет», рекомендуется реализовать положения приказа Минкомсвязи России от 16.06.2014 № 161 «Об утверждении требований к административным и организационным мерам, техническим и программно-аппаратным средствам защиты детей от информации, причиняющей вред их здоровью и (или) развитию» и нижеуказанный перечень административных мер защиты детей от информации, причиняющей вред их здоровью и (или) развитию:

1. Издавать нормативные локальные акты, направленные на обеспечение защиты детей от информации, причиняющей вред их здоровью и (или) развитию, и ознакомление с ними ответственных работников;

2. Осуществлять внутренний контроль за обновлением и соблюдением законодательства Российской Федерации о защите детей от информации, причиняющей вред их здоровью и (или) развитию, за соответствием применяемых административных и организационных мер защиты детей от информации, причиняющей вред их здоровью и (или) развитию, принципам и нормам информационной безопасности детей, включая критерии определения информационной продукции (информации), распространение которой на территории Российской Федерации запрещено или ограничено, установленные в действующих нормативных правовых актах Российской Федерации, в разъяснениях Верховного Суда Российской Федерации, а также общепризнанные нормы международного права, закрепленные в международных договорах Российской Федерации и рекомендациях международных организаций;

3. Обеспечивать оперативное рассмотрение претензий, жалоб или запросов органов власти, организаций и граждан Российской Федерации о нарушениях законодательства Российской Федерации о защите детей от информации, причиняющей вред их здоровью и (или) развитию, включая несоответствие применяемых административных и организационных мер защиты детей от информации, причиняющей вред их здоровью и (или) развитию, а также о наличии доступа детей к информации, запрещенной для распространения среди детей, и направление мотивированного ответа о результатах рассмотрения таких обращений, жалоб или претензий. В случае обращений со стороны органов власти, необходимо обеспечить предоставление информации и ответа в сроки, указанные в соответствующем обращении, но не позднее одного месяца с момента получения обращения;

4. Способствование выявлению правонарушений и преступлений, совершенных в отношении несовершеннолетних с использованием сети «Интернет», путем организации необходимых действий, указанных в запросах правоохранительных органов и органов прокуратуры;

5. Обеспечивать работу служб поддержки и исключения возможности трудоустройства в данные службы кандидатов, которые могут не подходить для работы, связанной с контактами с детьми: лишенные права заниматься педагогической деятельностью в соответствии со вступившим в законную силу приговором суда; имеющие или имевшие судимость, подвергающиеся или подвергавшиеся уголовному преследованию (за исключением лиц, уголовное преследование в отношении которых прекращено по реабилитирующим основаниям) за преступления против жизни и здоровья, свободы, чести и достоинства личности (за исключением незаконного помещения в психиатрический стационар, клеветы и оскорбления), половой неприкосновенности и половой свободы личности, против семьи и несовершеннолетних, здоровья населения и общественной нравственности, основ конституционного строя и безопасности государства, а также против общественной безопасности; имеющие неснятую или непогашенную судимость за умышленные тяжкие и особо тяжкие преступления; признанные недееспособными в установленном федеральным законодательством порядке:

6. Обеспечивать регулярный аудит систем мониторинга и фильтрации запрещенной для детей информации;

7. Оперативно удалять персональные данные детей, опубликованные на сайте либо сервисе с целью причинения вреда здоровью и (или) развитию ребенку или группе детей, чьи персональные данные были опубликованы, и направлять информацию о лицах, разместивших данную информацию для вышеуказанных целей, и лицах, участвующих в реализации вышеуказанных целей, в правоохранительные органы с целью привлечения данных лиц к ответственности.

Важным аспектом реализации административных мер защиты детей от информации, причиняющей вред их здоровью и (или) развитию, является повышение информационной компетентности в сфере кибербезопасности детей и их родителей (законных представителей).

В связи с этим рекомендуется организациям и физическим лицам, осуществляющим деятельность в информационно-телекоммуникационной сети «Интернет», реализовывать следующие меры:

1. Создавать и размещать на регулярной основе социальную рекламу и реализовывать другие просветительские меры, направленные на пропаганду информационной безопасности среди несовершеннолетних пользователей и их родителей (законных представителей);

2. Разместить информацию о контактах, включая интернет-ссылки и телефоны, соответствующих некоммерческих организаций и органов власти, осуществляющих деятельность в сфере обеспечения информационной безопасности детства;

3. Осуществлять сотрудничество с органами власти, образовательными организациями и некоммерческими организациями в целях повышения информационной культуры несовершеннолетних пользователей и их родителей (законных представителей) путем осуществления совместных просветительских проектов, создания образовательных ресурсов, разработки рекомендаций и материалов для обучения безопасной работы с сайтами или сервисами и в иных целях.

**Обмен информацией между пользователями**

В данную категорию входят интернет-ресурсы и технические программные решения, направленные на предоставление возможности двум и более пользователям в сети «Интернет» обмениваться информацией в любой форме, например, социальные сети, мессенджеры, сервисы электронной почты и другие, которым рекомендуется реализовать следующие меры:

1. Обеспечить внедрение функций приватности, оставив в результатах поиска внутри ресурса либо сервиса и (или) внешних поисковых систем следующую информацию из профилей зарегистрированных несовершенных пользователей: фамилия и имя, фотография (аватар) и дата рождения;

2. Обеспечить исключение из публичного доступа неограниченному кругу лиц персональных данных детей в виде геометок, номера телефона и информации об образовательном учреждении, в котором проходит обучение ребенок;

3. Включить в форму регистрации вопроса о возрасте пользователя и, в случае отметки пользователем о недостижении им совершеннолетия, предоставление возможности подключения родителей (законных представителей) для совместного управления аккаунтом;

4. Предоставить пользователям настройки предварительной модерации комментариев других пользователей перед публикацией в своем профиле;

5. Обеспечить внедрение функции, позволяющей ограничить взаимодействие детей с запрещенным для детей информационным контентом и включение данной функции по умолчанию;

6. Разработать механизм родительского контроля, предоставляющий возможность родителям отслеживать список друзей ребенка, его местонахождения и его активности;

7. Ограничить допуск детей в возрасте до 12 лет до каналов и сообществ, содержащих нежелательный контент для детей, и разработать механизмы предупреждения о нежелательном контенте для остальных возрастных групп до 18 лет в соответствии с возрастной классификацией информации, предусмотренной Федеральным законом от 29 декабря 2010 г. № 436-Ф3 «О защите детей от информации, причиняющей вред их здоровью и развитию»;

8. Исключить для несовершеннолетних пользователей рекламу, ориентированную на вовлечение детей в противоправные действия и в политическую деятельность, и рекламу нежелательного контента для детей;

9. Разработать функционал, позволяющий авторам при публикации и распространении контента для более двух лиц разместить возрастную маркировку «запрещено для детей», и обеспечить невозможность просмотра данного материал несовершеннолетними пользователями;

10. Разработать правила для физических лиц и юридических лиц об использовании сайта или сервиса в качестве канала распространения информации для более двух пользователей, объединенных в группы, каналы и другие формы распространения информации.

**Информационные сайты**

В данную категорию входят интернет-ресурсы и технические программные решения, предоставляющие пользователям сети «Интернет» в одностороннем порядке информацию общественного, политического, либо другого характера, которым рекомендуется реализовать следующие меры:

1. Разместить знак информационной продукции и (или) текстовое предупреждение об ограничении ее распространения среди детей, соответствующие одной из категорий информационной продукции, установленных частью 3 статьи 6 Федерального закона от 29 декабря 2010 г. № 436-ФЗ «О защите детей от информации, причиняющей вред их здоровью и развитию»;

2. До просмотра мультимедиа (видео, фотографии, комментарии и другого контента), в котором может содержаться запрещенная для детей информация, разместить текстовый или графический знак информационной продукции для предупреждения о недопустимости просмотра данного контента детьми;

3. При наличии функций, позволяющих пользователям обсуждать и комментировать контент, рядом с каждым сообщением должна быть предусмотрена функция жалобы в администрацию ресурса о нарушении законодательства в сфере информационной защиты детей.

Кроме этого, администрации информационного сайта рекомендовано обеспечивать контроль за распространяемой информацией как на собственном сайте, так и на других сайтах, используемых администрацией информационного сайта.

**Интернет-сервисы**

В данную группу входят интернет-ресурсы и технические программные решения, направленные на предоставление своим пользователям различных товаров и(или) услуг, например, интернет-магазины, приложения, игры и другие, которым рекомендуется реализовать следующие меры:

1. При продаже товаров и услуг, которые включают информационный контент, запрещенный для несовершеннолетних и отдельных возрастных категорий в соответствии с Федеральным законом от 29 декабря 2010 г. № 436-Ф3 «О защите детей от информации, причиняющей вред их здоровью и развитию», администрация интернет- сервиса обязана запросить дополнительную информацию о покупателе (Ф.И.О.; возраст, телефон) и, в случае недостижения пользователем возраста продажи либо непредоставления данной информации, отказать в продаже товара или оказания услуг;

2. При предоставлении товаров и услуг, ориентированных на взрослых, подробная информация о них должна быть недоступна. Краткая информация должна содержать возрастную маркировку, текстовое предупреждение о недопустимости просмотра данного товара или услуги до момента согласия пользователя об ответственности за последствия просмотра подробной информации;

3. Разработать методы родительского контроля, позволяющие родителям ознакомиться с историей оказанных их ребенку услуг или приобретенными им товарами, настраивать доступные ребенку категории товаров или услуг и ограничить возможности ребенка по получению ими возмездных или безвозмездных товаров, или услуг.

**Поисковые системы**

В данную группу входят интернет-ресурсы и технические программные решения, направленные на организацию поиска по запросу пользователя информации в сети «Интернет» и (или) информации в рамках интернет-ресурса или технического программного решения, на котором организован поиск информации, например, поисковые системы, системы поиска для сайтов и другие, которым рекомендуется реализовать следующие меры:

1. Разработать механизм предупреждения пользователей о нежелательном для детей контенте, выдающемся в результатах поиска;

2. Разработать механизм безопасного поиска, предназначенного для родителей (законных представителей) и позволяющего при включении ограничить допуск несовершеннолетних пользователей к нежелательному контенту;

3. Исключить из результатов поиска персональные данные детей в форме ссылок на аккаунты в социальных сетях;

4. Использовать средства контентной фильтрации для выявления запрещённой для детей информации.

**Ресурсы, содержащие информацию, запрещенную для детей**

В данную группу входят интернет-ресурсы и технические программные решения, публикующие и распространяющие информационный контент, запрещенный для детей в соответствии с Федеральным законом от 29 декабря 2010 г. №436-ФЭ «О защите детей от информации, причиняющей вред их здоровью и развитию» и отдельными законодательными актами Российской Федерации, которым рекомендуется реализовать следующие меры:

1. До ознакомления с информацией, публикуемой администрацией интернет-сервиса и запрещенной для детей в соответствии с Федеральным законом от 29 декабря 2010 г. № 436-ФЗ «О защите детей от информации, причиняющей вред их здоровью и развитию» и отдельными законодательными актами Российской Федерации, пользователь должен пройти регистрацию, указав Ф.И.О., номер телефона и возраст. Дальнейший доступ к информации должен быть разрешен только для совершеннолетних граждан, и, в случае не достижения пользователем совершеннолетнего возраста, администрация интернет - ресурса обязана отказать в регистрации и ограничить самостоятельный доступ к сайту.

Образовательным организациям и физическим лицам рекомендуется исключить рекламу данных Интернет-ресурсов или технических программных решении, включая размещение информации об их работе, контенте и другой информации в сети «Интернет», для неограниченного круга лиц, среди которых могут быть несовершеннолетние пользователи.

**Примерные направления работы образовательных организаций**

**ОАО «РЖД**» **направленных на профилактику рисков и угроз для детей, связанных с использованием современных информационных технологий информационно-телекоммуникационной сети «Интернет».**

Проблема информационной безопасности при организации образовательного процесса – одна из самых актуальных на современном этапе в любой образовательной организации любой ступени обучения (дошкольные образовательные учреждения, общеобразовательные школы и пр.).

Растёт количество угроз из сети «Интернет», соответственно реалиям времени меняются и методы обеспечения информационной безопасности учебного процесса.

Направления деятельности по обеспечению информационной безопасности образовательного процесса предполагают следующие мероприятия:

* по формированию и расширению компетентности работников сферы образования в области медиабезопасного поведения детей и подростков;
* по организации просветительской работы среди обучающихся;
* по созданию педагогических условий обеспечения информационной безопасности, обучающихся и информационной открытости;
* по организации просветительской работы с родителями (законными представителями).

**Нормативно-правое обеспечение** является основой образовательного учреждения по всем направлениям. В образовательном учреждении должен быть сформирован пакет нормативно-правовой документации федерального, регионального и муниципального учрежденческого уровней по вопросам информационной безопасности.

К таким документам относятся документы по контентной фильтрации, по обработке персональной информации, положения и регламенты по работе в сети Интернет как педагогических работников, так и несовершеннолетних, различные положения об организации профилактической работы по медиабезопасности, о формах профилактической работы с детьми и родителями по Интернет- безопасности, правила безопасного поведения в сети образовательном учреждении приказами должны быть назначены лица, ответственные за контентную фильтрацию, за работу с персональными данными, за организацией работы школьников в сети Интернет и т.д.

В **организационном плане** по обеспечению информационной медиабезопасности в образовательном учреждении должен выполняться ряд мер технико-технологической направленности:

* установка только лицензионного программного обеспечения,
* подключение к системе контентной фильтрации;
* установка антивирусных программ,
* установка и настройка программ-фильтров, брандмауэров.

К **организационным мероприятиям** относятся:

1. Разработка и реализация правил Интернет-безопасности, с привлечением заинтересованных лиц:

* Руководителя учреждения,
* Педагогических работников (воспитатели, учителя, специалисты),
* Самих обучающихся и их родителей,
* Поставщиков услуг интернета.

2. Организация работы несовершеннолетних в сети «Интернет» по расписанию с ограничением по времени под наблюдением педагогических работников,

3. Регулярная проверка принимаемых мер в области Интернет безопасности в образовательном учреждении.

Для организации **профилактической работы** по медиабезопасности с детьми и родителями сам педагогический работник должен знать проблемы и опасности, которые подстерегают пользователя в сети «Интернет», и быть готов дать рекомендации по решению данных проблем.

Для организации профилактических мер в образовательном учреждении необходимо периодически проводить мониторинг, диагностику проблем по Интернет-безопасности среди детей и родителей. Данный мониторинг и разъяснительную работу можно проводить на сайте образовательного учреждения или в Интернет- проекте «Дневник.ру». В этом проекте реализованы функции школьного модератора, в обязанности которого входит модерация нежелательного содержания в сети проекта и есть возможность применять действенные санкции к нарушителям правил пользования интернетом. В Интернет- проекте «Дневник.ру» можно организовать виртуальные мероприятия с родителями по вопросам Интернет-безопасности, разместить рекомендации в электронном виде.

В аспекте **программно-методического обеспечения** образовательном учреждении может быть разработана программа (раздел, модуль комплексной программы по профилактике девиантного поведения детей), в которую должны быть включены темы по медиабезопасности, о безопасном поведении в сети Интернет. Такие же темы и проблемы могут быть включены в программы воспитательной работы образовательного учреждения.

Рекомендуемая тематика для организации профилактической деятельности:

* нежелательная информация в Интернете, как ее избежать;
* проблемы достоверности информации в Интернете, как проверить достоверность информации;
* социальные сети: опасности и правила поведения в социальных сетях;
* кибермошенничества, как избежать кибермошенников;
* киберхулиганство, киберзапугивание, правила поведения в опасной виртуальной ситуации;
* вредоносные программы, методы борьбы с ними;
* полезные ссылки, ресурсы, сервисы в сети «Интернет».

Информационная безопасность в сети «Интернет» может обсуждаться на родительских собраниях, классных часах, во время уроков информатики, социологии, ОБЖ, гражданского права и др. В образовательном учреждении рекомендуется проводить день медиабезопасности, уроки по Интернет-безопасности, внеклассные мероприятия и т.п.

Во время мероприятий по медиабезопасности следует ознакомить обучающихся:

* с правилами ответственного и безопасного поведения современной информационной среде, способах защиты от противоправных посягательств в сети Интернет и мобильной (сотовой) связи;
* с информацией о необходимости критического отношения к сообщениям в СМИ (в т.ч. электронных), мобильной (сотовой) связи, признаках отличия достоверных сведений от недостоверных, способах нейтрализации вредной и опасной для детей информации, распознавания признаков злоупотребления доверчивостью;
* с правилами общения в социальных сетях (сетевой этикет);
* с адресами помощи в случае интернет- угрозы, номером всероссийского детского телефона доверия (8-800-2500015).

**Основные формы и направления мероприятий в образовательной организации** **направленные на профилактику рисков и угроз для детей, связанных с использованием современных информационных технологий информационно-телекоммуникационной сети «Интернет».**

1. Мероприятия по формированию и расширению компетентности работников сферы образования в области медиабезопасного поведения детей и подростков.

*Например: Педагогические советы, совещания, лектории, семинары, круглые столы, школьные методические объединения профилактической работы с учащимися и семьями по медиабезопасному поведению в сети интернет», «Безопасность подростков в социальных сетях», «Способы формирования антиманипулятивного «Кибербулинг: профилактика в среде учащихся», «Безопасный Интернет для детей и подростков: социальные и психологические аспекты», «Что такое «Цифровая репутация».*

2. Мероприятия по организации просветительской работы среди обучающихся.

*Например: Классные часы, лекции, видеоролики, квест-игры, интерактивные квесты, конкурсы, интерактивные занятия: «Безопасность в сети Интернет», «Игромания – последствия зависимости», «Общие рекомендации по безопасной работе в интернете», «Польза и вред социальных сетей», «Законодательные меры за противоправные действия в сети Интернет», участие в конференции «Start-IT», медиа-презентации на переменах «Безопасный интернет», проведение дня IT- знаний, участие во Всероссийской контрольной работе по информационной безопасности на сайте* [*http://единыйурок.дети*](http://единыйурок.дети) *, участие во Всероссийской добровольной просветительской интернет-акции «Безопасность детей в сети Интернет», проведение Единых уроков по безопасности в сети Интернет, тренажёры по* *безопасности в интернете.*

3. Мероприятия по созданию педагогических условий обеспечения информационной безопасности, обучающихся и информационной открытости.

*Например: Педагогические советы на темы «Информационная безопасность», «Регламент доступа учащихся к сети Интернет», осуществление контент фильтрации, мониторинг качества системной контент-фильтрации и применения организационно-административных мероприятий, направленных на защиту детей от негативной информации, проведение инструктажей, размещение информационных материалов на внутренних онлайн-ресурсах, мониторинг «Информационная безопасность», организация свободного доступа обучающихся и учителей к высокоточным и сетевым образовательным ресурсам, в том числе к системе современных материалов по всем предметам, размещение ссылок на официальных сайтах центров по проблемам информационной безопасности для всех участников образовательного процесса, осуществляется работа Общественных советов по регламентации доступа к сети Интернет, выполнение комплекса мер по антивирусной защите компьютерной техники, контроль за использованием лицензионного программного обеспечения в административной и образовательной деятельности.*

4. Мероприятия по организации просветительской работы родителями (законными представителями).

*Например: Родительские собрания, лектории для родителей, консультации, памятки по темам «Безопасность в сети Интернет», «Влияние Интернета на личность ребёнка», «Здоровье и безопасный Интернет», «Безопасные покупки в Интернете», «Правила работы с компьютером и телефоном», «Управление безопасностью детей в Интернете», консультирование родителей по вопросам защиты детей от распространения вредной для них информации, информационные стенды (рубрики «Советы родителям», «Чем занять ребенка до лет за компьютером?»), участие во Всероссийской добровольной просветительской интернет-акции «Безопасность детей в сети Интернет».*

Приложение 1.

**Рекомендуемые информационные ресурсы**

* Брошюра МВД России «Безопасный интернет» <http://www.mvd.ru/userfiles/broshyura_k_01_02_2012.pdf>
* Безопасный Интернет от Билайн <http://safe.beeline.ru/index.wbp>
* Безопасный интернет от Мегафона <http://stopfraud.megafon.ru/parents/>
* Безопасный Интернет от МТС <http://www.mts.ru/help/useful_data/safety/>
* Безопасный интернет от microsoft <http://www.microsoft.com/ru-ru/security/default.aspx>
* Брошюра от microsoft «Безопасность детей в интернете» <http://www.ifap.ru/library/book099.pdf>
* Видео-выступление Ефимовой О.И. доцента, кандидата психологических наук, с.н.с. ФГБНУ «Центр защиты прав и интересов детей» Психологическая газета. <http://wwwpsy.su>
* Влияние соцсетей на поведение подростков представлено на сайте. <http://www62ru.ru/news1.php> Спасение детей от кибер преступлений.
* Дети России онлайн <http://detionline.com/helpline/rules/parents>
* «Новая газета» <http://www.novayagazeta.ru> рассказывает о целой серии закрытых групп во «ВКонтакте», организующих самоубийства подростков посредством психологического давления и зловещих квестов.
* Сайт ФГБНУ «Центр защиты прав и интересов детей». На специализированной странице сайта представлена информация по профилактике суицидального поведения несовершеннолетних. <http://wwwfcprc.ru>
* Сайт «Я – родитель» На сайте представлены полезные советы, указания и подсказки для родителей по воспитанию, обучению и развитию детей. Решение психологических проблем детей <http://www.ya-roditel.ru>
* Памятка для родителей «Куда обратиться, если есть подозрения о нахождении ребенка в «группах смерти»?» <http://www.ya-roditel.ru/parents/ig/gruppy-smerti-chto-nuzhno-znat-o-nikh-roditelyam>
* Научно-методический журнал «Образование личности» <http://www.ol-journal.ru>
* Научно-практический журнал «Профилактика зависимостей» <http://профилактика-зависимостей.рф>
* Центр безопасного Интернета в России, горячая линия по безопасному Интернету <http://www.saferunet.ru/>

Приложение 2.

**Рекомендации по проведению родительских собраний и бесед с**

 **родителями, направленных на профилактику интернет-рисков**

**и угроз жизни несовершеннолетних**

* Перед проведением собрания или беседы педагогам необходимо внимательно ознакомиться с материалами, представляемыми родителям на собрании (сценарием, дополнительными материалами, презентацией), прояснить все вопросы, в случае необходимости обратиться за консультацией к представителю администрации, психологу или другому специалисту.
* К собранию необходимо подготовить информацию (адреса и телефоны) региональных организаций, в которые родители могут обратиться в трудной ситуации, в ситуации угрозы жизни подростка: региональных служб и центров оказания помощи семье и детям, региональных телефонов доверия, ППМС-центров, службах психологической, психиатрической помощи, подразделениях и службах департаментов социальной защиты, подразделениях по делам несовершеннолетних и т.п.
* Для участия в собрании могут быть привлечены специалисты, психологи, медицинские работники.
* Собрания лучше проводить в классе/группе или по возрастным параллелям. Беседы с родителями по конкретным ситуациям должны носить только индивидуальный характер.
* При проведении родительских собраний и бесед с родителями важно учитывать эмоциональную значимость темы. Не должны обсуждаться конкретные случаи, имеющие место в классах или в знакомом окружении.
* Родителей необходимо проинформировать о «вбросах» недостоверной информации, уведомить их о необходимости и возможности проверки такой информации. Ни в коем случае нельзя запугивать родителей и самих подростков угрозами суицида и склонением к суицидальному поведению.
* Родителям учеников необходимо дать информацию о необходимости родительского контроля времени пребывания ребенка в Интернете и использованием ребенком интернет-ресурсов, а также о мерах защиты от интернет-рисков, которые они могут применить в домашних условиях и установить по договору с Провайдером, предоставляющим услуги интернет-связи.

Приложение 3.

**В качестве средств защиты родителям могут быть представлены популярные программные средства, которые помогут защитить ребенка от нежелательной информации в Сети, в частности:**

* iProtectYouPro — программа-фильтр Интернета позволяет родителям ограничивать по разным параметрам сайты, просматриваемые детьми ресурсы.
* KidsControl – контроль времени, которое ребенок проводит в Интернете.
* Mipko Time Sheriff предназначен для контроля времени, проводимого вашими детьми за компьютером или работы с конкретными программами и сайтами.
* NetPolice Lite выполняет функцию родительского контроля, запрещая детям посещать сайты определенных категорий (сайты для взрослых, ненормативная лексика и т.п.).
* ИНТЕРНЕТ ЦЕНЗОР — программа содержит уникальные вручную проверенные «белые списки», включающие все безопасные сайты Рунета и основные иностранные ресурсы. Программа надежно защищена от взлома и обхода фильтрации.

Приложение 4.

**Куда надо обращаться в суицидоопасной ситуации**

* Всероссийский Детский телефон доверия: 8-800-2000-122 (бесплатно, круглосуточно).
* Психологическое консультирование, экстренная и кризисная психологическая помощь для детей в трудной жизненной ситуации, подростков и их родителей имеется в каждом регионе.
* Горячая линия «Ребенок в опасности» Следственного комитета РФ. Дети, их родители, а также все неравнодушные граждане, обладающие информацией о совершенном или готовящемся преступлении против несовершеннолетнего или малолетнего ребенка, могут позвонить по бесплатному, круглосуточному номеру телефона 8-800-200-19-10 из московского региона России.

Приложение 5.

**Примерный план мероприятий**

**по обеспечению информационной безопасности и безопасному использованию сети «Интернет»**

 **в образовательных организациях** **ОАО «РЖД»**

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| № | Направления деятельности и наименование мероприятий | Ответственные  | Сроки | Ожидаемые результаты |
| **1. Организационно-правовые механизмы защиты несовершеннолетних от информации причиняющей им вред** |
| 1.1. | Организация контроля обеспечением защиты детей от распространения информации, причиняющей вред их здоровью и развитию, в соответствии действующим законодательством. | Руководитель ОО,заместитель руководителя ОО, информатик/программист | в течение года | охват всех обучающихся |
| 1.2. | Приведение локальных актов ОО, регламентирующих работу в сети Интернет, в соответствие с действующим законодательством.  | Заместитель руководителя ОО, информатик/программист | начало учебного года | Локальные регламентирующие работу в сети Интернет, приведены соответствие с действующим законодательством. |
| 1.3. | Проведение контроля функционирования интернет-ресурсов ОО. | Информатик/программист | 1 раз в неделю | 100% обеспечение услуги доступа в сеть Интернет школе с обеспечением контент-фильтрации Интернет - трафика |
| 1.4. | Организация профилактических мероприятий с родителями обучающимися по вопросам информационной безопасности. | Заместитель руководителя ОО, педагогические работники | в течение года | 100% ознакомление родителей и обучающихся с информацией по медиабезопасности  |
| 1.5. | Осуществление педагогами контроля при работе обучающихся в сети Интернет. | Педагогические работники | в течение года | Во время работы 100% осуществление контроля стороны педагогов при работе обучающихся в сети Интернет. |
| **2. Информационное обеспечение и внедрение систем исключения доступа к информации, несовместимой с задачами****образования и воспитания обучающихся** |
| 2.1. | Установка, настройка, проверка работоспособности и обеспечение бесперебойного функционирования программных средств контентной фильтрации, обеспечивающих исключение доступа обучающихся к ресурсам сети Интернет, содержащим информацию, несовместимую с задачами образования и воспитания учащихся. | Информатик/программист | на начало учебного года | 100% обеспечение услуги доступа в сеть Интернет школе с обеспечением контент-фильтрации Интернет - трафика |
| 2.2. | Обновление раздела «Информационная безопасность» официального сайта ОО обеспечению информационной безопасности обучающихся при использовании ресурсов сети Интернет. | Заместитель руководителя ОО | на начало учебного года | Регулярное обновление раздела «Информационная безопасность» официального сайта ОО обеспечению информационной безопасности учащихся при использовании ресурсов сети Интернет. |
| 2.3. | Мониторинг исключения доступа к Интернет-ресурсам, несовместимым с целями и задачами образования и воспитания обучающихся. | Информатик/программист | ежеквартально | 100% обеспечение услуги доступа в сеть Интернет школе с обеспечением контент-фильтрации Интернет – трафика  |
| **3. Профилактика у детей и подростков интернет-зависимости и правонарушений с использованием информационно-телекоммуникационных технологий, формирование у несовершеннолетних навыков ответственного и безопасного поведения в современной информационно-телекоммуникационной среде** |
| 3.1. | Включение в план воспитательной работы ОО и организация мероприятий:- уроки, внеурочные занятия по теме «Информационная безопасность»;- обучающие мероприятия для педагогов по вопросам обеспечения организационных исключения доступа к Интернет- ресурсам, несовместимым с целями и задачами образования и воспитания;- родительские собрания по вопросам профилактики экстремистских проявлений среди информационного противодействия терроризму в социальных блогах и на форумах | Заместитель руководителя ОО, педагогические работники | в течение года | 100% выполнение плана воспитательных мероприятий по теме «Информационная безопасность» |
| 3.2. | Участие в методических мероприятиях по созданию надежной системы защиты детей противоправного контента образовательной среде школы и дома, по вопросам компетентности учащихся. | Заместитель руководителя ОО, педагогические работники | в течение года | По плану 100% обеспечение услуги доступа в сеть Интернет ОО с обеспечением контент-фильтрации Интернет - трафика |
| **4. Информационное просвещение граждан о возможности защиты несовершеннолетних от информации, причиняющей вред их****здоровью и развитию** |
|  | Включение в повестку совещаний педагогических работников ОО, родительских собраний вопросов обеспечения информационной безопасности детей при использовании ресурсов сети Интернет, профилактики у детей и подростков интернет-зависимости, игровой зависимости правонарушений с использованием информационно-телекоммуникационных технологий, формирование несовершеннолетних навыков ответственного и безопасного поведения в современной информационно-телекоммуникационной среде. | Заместитель руководителя ОО, педагогические работники | в течение года | Совещания участников образовательного процесса о возможности защиты детей от информации, причиняющей вред их здоровью |
|  | Поддержание в актуальном состоянии на официальном сайте образовательной организации раздела «Информационная безопасность», публикация материалов по обеспечению информационной безопасности детей при использовании ресурсов сети Интернет. | Заместитель руководителя ОО | в течение года | Создание или актуализация страницы «Информационная безопасность» |
|  | Размещение на сайте ОО ссылок на электронные адреса по проблемам информационной безопасности для всех участников образовательного процесса | Заместитель руководителя ОО | в течение года | Повышение грамотности проблемам информационной безопасности всех участников образовательного процесса |
|  | Беседы с использованием материалов Интернет-ресурсов: «Интернет среди нас»; «Я и мои виртуальные друзья»; «Интернет в моей семье»; «Мой Интернет»; «Мой социум Интернете»; «Интернет и моя будущая профессия»; «Интернет и мое G здоровье». | Заместитель руководителя ОО | в течение года | 100% охват участников образовательного процесса занятиями по медиабезопасности. |