Красноярский краевой институт повышения квалификации
и профессиональной переподготовки работников образования

ОБЕСПЕЧЕНИЕ МЕДИАБЕЗОПАСНОСТИ В ОБРАЗОВАТЕЛЬНОЙ ОРГАНИЗАЦИИ

Методические рекомендации

Красноярск–2023

ББК 74.204
О–13

Рецензенты

Т.А. Кондратюк, доцент кафедры информационных технологий обучения и непрерывного образования СФУ, кандидат педагогических наук, доцент

Н.В. Бекузарова, доцент кафедры информационных технологий обучения и непрерывного образования СФУ, кандидат педагогических наук, доцент

О–13 **Обеспечение медиабезопасности в образовательной организации:** методические рекомендации / сост. И.В. Хабарова. – Красноярск, 2023. – 48 с.

ББК 74.204

В методических рекомендациях раскрыты основные понятия, касающиеся информационной безопасности детей, использующих Интернет и различные виды телекоммуникаций. Описаны способы защиты информации в медиапространстве, рассмотрены актуальные нормативные документы по теме обеспечения медиабезопасности в образовательной организации.

В пособии обозначены условия, способы и инструменты создания безопасной информационной среды в образовательной организации.

Издание адресовано педагогам, методистам, специалистам образовательных организаций.

Печатается по решению редакционно-издательского совета
Красноярского краевого института повышения квалификации
и профессиональной переподготовки работников образования

СОДЕРЖАНИЕ

Предисловие

Современному педагогу необходимо владеть умением разрабатывать (осваивать) и применять современные психолого-педагогические технологии, основанные на знании законов развития личности и поведения в реальной и виртуальной среде, выстраивать сотрудничество с другими педагогическими работниками и другими специалистами в решении воспитательных задач.

В образовательной организации важным направлением деятельности является организация правового просвещения и распространения информации о правах ребёнка, адаптированной для детей, родителей, учителей, специалистов, работающих с детьми и в интересах детей, через средства массовой информации, информационно-телекоммуникационную сеть Интернет.

В интернет-пространстве информация распространяется быстро благодаря техническим возможностям. Школьник, включенный в процесс познания, оказывается не защищённым от потоков информации. Пропаганда жестокости, насилия, недостаток цензуры является не только социальной, но и педагогической проблемой. Необходимо направить все усилия на защиту детей от информации, причиняющей вред их здоровью и развитию. Просвещение подрастающего поколения, знание ребёнком элементарных правил отбора информации, а также умение ею пользоваться способствует развитию системы защиты прав детей. Обеспечение информационной безопасности детей, защита физического, умственного, нравственного развития несовершеннолетних – это задача и семейного, и школьного воспитания. Следовательно, возникает необходимость повышения уровня компетентности педагогов в области обеспечения медиабезопасности обучающихся.

1. Нормативно-правовые основания обеспечения информационной безопасности обучающихся

Безопасность в медиапространстве на международном уровне гарантируется следующими нормативно-правовыми документами:

- Конвенция о правах ребёнка (одобрена Генеральной Ассамблеей ООН 20.11.1989).
- Решение № 276/1999/ЕС Европейского парламента и Совета Европейского Союза «О принятии Многолетнего плана действий Сообщества по содействию более безопасному использованию сети Интернет и новых онлайновых технологий путем борьбы с незаконным и вредным контентом, прежде всего в сфере защиты детей и несовершеннолетних» (Вместе с «Многолетним планом действий Сообщества и средствами его реализации», «Примерным распределением расходов») (Принят в г. Брюсселе 25.01.1999) (с изм. и доп. от 21.04.2004).

- Декларация о свободе обмена информацией в Интернете (принята Комитетом Министров Совета Европы от 28 мая 2003 г. на 840-м заседании заместителей Министров).
- Рекомендация № 2006/952/ЕС Европейского парламента и Совета Европейского Союза «О защите несовершеннолетних и человеческого достоинства, а также о праве на ответ в отношении конкурентоспособности европейской аудиовизуальной и онлайновой индустрии информационных услуг». (Вместе с «Индикативным руководством по реализации на национальном уровне мер, предусмотренных внутренним законодательством или практикой») (Принята в г. Брюсселе 20.12.2006).

Законодательство Российской Федерации о защите детей от информации, причиняющей вред их здоровью и (или) развитию, состоит из Конституции Российской Федерации, Федерального закона от 29.12.2010 № 436-ФЗ «О защите детей от информации, причиняющей вред их здоровью и развитию», других федеральных законов и принимаемых в соответствии с ними иных нормативных правовых актов. Информационная безопасность детей в Российской Федерации обеспечиваются следующими нормативно-правовыми документами:

- Федеральный закон от 24.07.1998 N 124-ФЗ (ред. от 27.12.2018) «Об основных гарантиях прав ребёнка в Российской Федерации, который декларирует, что государственная политика в интересах детей является приоритетной и основана на следующих принципах:
- *законодательное обеспечение прав ребёнка;*
- *поддержка семьи в целях обеспечения обучения, воспитания, отдыха и оздоровления детей, защиты их прав, подготовки их к полноценной жизни в обществе;*
- *ответственность юридических лиц, должностных лиц, граждан за нарушение прав и законных интересов ребёнка, причинение ему вреда;*
- *поддержка общественных объединений и иных организаций, осуществляющих деятельность по защите прав и законных интересов ребёнка.*
- Федеральный закон от 29.12.2012 № 273-ФЗ «Об образовании в Российской Федерации», регулирующий общественные отношения, возникающие в сфере образования в связи с реализацией права на образование, обеспечением государственных гарантий прав и свобод человека в сфере образования и созданием условий для реализации права на образование (далее – отношения в сфере образования).
- Федеральный закон от 27.07.2006 № 152-ФЗ «О персональных данных», целью которого является обеспечение защиты прав и свобод человека и гражданина при обработке его персональных данных, в том числе защиты прав на неприкосновенность частной жизни, личную и семейную тайну.

- Федеральный закон от 27.07.2006 № 149-ФЗ «Об информации, информационных технологиях и о защите информации», регулирующий отношения, возникающие при:

1) осуществлении права на поиск, получение, передачу, производство и распространение информации;

2) применении информационных технологий;

3) обеспечении защиты информации.

Федеральный закон от 28.12.2010 № 390-ФЗ (ред. от 09.11.2020) «О безопасности», определяющий основные принципы и содержание деятельности по обеспечению безопасности государства, общественной безопасности, экологической безопасности, безопасности личности, иных видов безопасности, предусмотренных законодательством Российской Федерации.

Федеральный закон от 29.12.2010 № 436-ФЗ (ред. от 01.07.2021) «О защите детей от информации, причиняющей вред их здоровью и развитию» регулирует отношения, связанные с защитой детей от информации, причиняющей вред их здоровью и (или) развитию, в том числе от такой информации, содержащейся в информационной продукции. Основные понятия, касающиеся медиабезопасности, используемые в ФЗ «О защите детей от информации, причиняющей вред их здоровью и развитию» от 29.12.2010 № 436-ФЗ»:

– *доступ детей к информации – возможность получения и использования детьми свободно распространяемой информации;*

– *информационная безопасность детей – состояние защищенности детей, при котором отсутствует риск, связанный с причинением информацией вреда их здоровью и (или) физическому, психическому, духовному, нравственному развитию;*

– *информационная продукция для детей – информационная продукция, соответствующая по тематике, содержанию и художественному оформлению физическому, психическому, духовному и нравственному развитию детей;*

– *информация, причиняющая вред здоровью и (или) развитию детей, – информация (в том числе содержащаяся в информационной продукции для детей), распространение которой среди детей запрещено или ограничено в соответствии с настоящим Федеральным законом;*

– *информация порнографического характера – информация, представляемая в виде натуралистических изображения или описания половых органов человека и (или) полового сношения либо сопоставимого с половым сношением действия сексуального характера, в том числе такого действия, совершаемого в отношении животного;*

– *классификация информационной продукции – распределение информационной продукции в зависимости от её тематики, жанра, содержания*

и художественного оформления по возрастным категориям детей в порядке, установленном настоящим Федеральным законом;

– *натуралистические изображение или описание – изображение или описание в любой форме и с использованием любых средств человека, животного, отдельных частей тела человека и (или) животного, действия (бездействия), события, явления, их последствий с фиксированием внимания на деталях, анатомических подробностях и (или) физиологических процессах;*

– *оборот информационной продукции – предоставление и (или) распространение информационной продукции, включая её продажу (в том числе распространение по подписке), аренду, прокат, раздачу, выдачу из фондов общедоступных библиотек, публичный показ, публичное исполнение (в том числе посредством зрелищных мероприятий), распространение посредством эфирного или кабельного вещания, информационно-телекоммуникационных сетей, в том числе сети Интернет, и сетей подвижной радиотелефонной связи.*

В соответствии со статьёй 4 пункт 2 436-ФЗ к полномочиям органов государственной власти субъектов Российской Федерации в сфере защиты детей от информации, причиняющей вред их здоровью и (или) развитию, относятся разработка и реализация перечня региональных мероприятий, направленных на обеспечение информационной безопасности детей, производство информационной продукции для детей и оборот информационной продукции, а также иные полномочия, установленные настоящим Федеральным законом.

Ниже приведём перечень видов информации, причиняющей вред здоровью и (или) развитию детей, в соответствии со статьей 5 ФЗ «О защите детей от информации, причиняющей вред их здоровью и развитию»:

1. *К информации, причиняющей вред здоровью и (или) развитию детей, относится:*

1) информация, предусмотренная частью 2 настоящей статьи и запрещенная для распространения среди детей;

2) информация, которая предусмотрена частью 3 настоящей статьи с учетом положений статей 7–10 настоящего Федерального закона и распространение которой среди детей определенных возрастных категорий ограничено.

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

1) побуждающая детей к совершению действий, представляющих угрозу их жизни и (или) здоровью, в том числе к причинению вреда своему здоровью, самоубийству, либо жизни и (или) здоровью иных лиц, либо направленная на склонение или иное вовлечение детей в совершение таких действий (в ред. Федерального закона от 18.12.2018 № 472-ФЗ);

2) способная вызвать у детей желание употребить наркотические средства, психотропные и (или) одурманивающие вещества, табачные изделия, никотинсодержащую продукцию, алкогольную и спиртосодержащую продукцию, принять участие в азартных играх, заниматься проституцией, бродяжничеством или попрошайничеством (в ред. Федеральных законов от 29.06.2015 № 179-ФЗ, от 31.07.2020 № 303-ФЗ);

3) обосновывающая или оправдывающая допустимость насилия и (или) жестокости либо побуждающая осуществлять насильственные действия по отношению к людям или животным, за исключением случаев, предусмотренных настоящим Федеральным законом;

3.1) содержащая изображение или описание сексуального насилия (п. 3.1 введен Федеральным законом от 01.05.2019 № 93-ФЗ);

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

5) оправдывающая противоправное поведение;

6) содержащая нецензурную брань;

7) содержащая информацию порнографического характера;

8) о несовершеннолетнем, пострадавшем в результате противоправных действий (бездействия), включая фамилии, имена, отчества, фото- и видеоизображения такого несовершеннолетнего, его родителей и иных законных представителей, дату рождения такого несовершеннолетнего, аудиозапись его голоса, место его жительства или место временного пребывания, место его учебы или работы, иную информацию, позволяющую прямо или косвенно установить личность такого несовершеннолетнего.

3. *К информации, распространение которой среди детей определенных возрастных категорий ограничено, относится информация:*

1) представляемая в виде изображения или описания жестокости, физического и (или) психического насилия (за исключением сексуального насилия), преступления или иного антиобщественного действия;

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

3) представляемая в виде изображения или описания половых отношений между мужчиной и женщиной;

4) содержащая бранные слова и выражения, не относящиеся к нецензурной брани.

В соответствии со статьей 6 436-ФЗ осуществляется классификации информационной продукции (таблица 1).

Классификация информационной продукции осуществляется её производителями и (или) распространителями самостоятельно (в том числе с

участием эксперта, экспертов и (или) экспертных организаций, отвечающих требованиям статьи 17 настоящего Федерального закона) до начала её оборота на территории Российской Федерации.

2. При проведении исследований в целях классификации информационной продукции оценке подлежат:

1) её тематика, жанр, содержание и художественное оформление;

2) особенности восприятия содержащейся в ней информации детьми определенной возрастной категории;

3) вероятность причинения содержащейся в ней информацией вреда здоровью и (или) развитию детей.

3. Классификация информационной продукции осуществляется в соответствии с требованиями настоящего Федерального закона по следующим категориям информационной продукции:

1) информационная продукция для детей, не достигших возраста шести лет;

2) информационная продукция для детей, достигших возраста шести лет;

3) информационная продукция для детей, достигших возраста двенадцати лет;

4) информационная продукция для детей, достигших возраста шестнадцати лет;

5) информационная продукция, запрещенная для детей (информационная продукция, содержащая информацию, предусмотренную частью 2 статьи 5 настоящего Федерального закона).

4. Классификация информационной продукции, предназначенной и (или) используемой для обучения и воспитания детей в организациях, осуществляющих образовательную деятельность по реализации основных общеобразовательных программ, образовательных программ среднего профессионального образования, дополнительных общеобразовательных программ, осуществляется в соответствии с настоящим Федеральным законом и законодательством об образовании.

5. Классификация фильмов осуществляется в соответствии с требованиями настоящего Федерального закона и законодательства Российской Федерации о государственной поддержке кинематографии.

6. Сведения, полученные в результате классификации информационной продукции, указываются её производителем или распространителем в сопроводительных документах на информационную продукцию и являются основанием для размещения на ней знака информационной продукции и для её оборота на территории Российской Федерации (в ред. Федерального закона от 28.07.2012 № 139-ФЗ).

Таблица 1

Классификация информационной продукции для детей

Федеральный закон от 29.12.2010 № 436-ФЗ (ред. от 01.07.2021) «О защите детей от информации, причиняющей вред их здоровью и развитию»		
Статья	**Название**	**Классификация информационной продукции**
Статья 7	Информационная продукция для детей, не достигших возраста шести лет	К информационной продукции для детей, не достигших возраста шести лет, может быть отнесена информационная продукция, содержащая информацию, не причиняющую вреда здоровью и (или) развитию детей (в том числе информационная продукция, содержащая оправданные её жанром и (или) сюжетом эпизодические ненатуралистические изображение или описание физического и (или) психического насилия (за исключением сексуального насилия) при условии торжества добра над злом и выражения сострадания к жертве насилия и (или) осуждения насилия)
Статья 8	Информационная продукция для детей, достигших возраста шести лет	К допускаемой к обороту информационной продукции для детей, достигших возраста шести лет, может быть отнесена информационная продукция, предусмотренная статьей 7 настоящего Федерального закона, а также информационная продукция, содержащая оправданные её жанром и (или) сюжетом: 1) кратковременные и ненатуралистические изображение или описание заболеваний человека (за исключением тяжелых заболеваний) и (или) их последствий в форме, не унижающей человеческого достоинства; 2) ненатуралистические изображение или описание несчастного случая, аварии, катастрофы либо ненасильственной смерти без демонстрации их последствий, которые могут вызывать у детей страх, ужас или панику; 3) не побуждающие к совершению антиобщественных действий и (или) преступлений эпизодические изображение или описание этих действий и (или) преступлений при условии, что не обосновывается и не оправдывается их

		допустимость и выражается отрицательное, осуждающее отношение к лицам, их совершающим
Статья 9	Информационная продукция для детей, достигших возраста двенадцати лет	К допускаемой к обороту информационной продукции для детей, достигших возраста двенадцати лет, может быть отнесена информационная продукция, предусмотренная статьей 8 настоящего Федерального закона, а также информационная продукция, содержащая оправданные её жанром и (или) сюжетом: 1) эпизодические изображение или описание жестокости и (или) насилия (за исключением сексуального насилия) без натуралистического показа процесса лишения жизни или нанесения увечий при условии, что выражается сострадание к жертве и (или) отрицательное, осуждающее отношение к жестокости, насилию (за исключением насилия, применяемого в случаях защиты прав граждан и охраняемых законом интересов общества или государства); 2) изображение или описание, не побуждающие к совершению антиобщественных действий (в том числе к потреблению алкогольной и спиртосодержащей продукции, участию в азартных играх, занятию бродяжничеством или попрошайничеством), эпизодическое упоминание (без демонстрации) наркотических средств, психотропных и (или) одурманивающих веществ, табачных изделий или никотинсодержащей продукции при условии, что не обосновывается и не оправдывается допустимость антиобщественных действий, выражается отрицательное, осуждающее отношение к ним и содержится указание на опасность потребления указанных продукции, средств, веществ, изделий (в ред. Федеральных законов от 29.06.2015 N 179-ФЗ, от 31.07.2020 N 303-ФЗ) (см. текст в предыдущей редакции); 3) не эксплуатирующие интереса к сексу и не носящие возбуждающего или оскорбительного характера эпизодические ненатуралистические изображение или описание половых отношений между мужчиной и женщиной, за

		исключением изображения или описания действий сексуального характера
Статья 10	Информационная продукция для детей, достигших возраста шестнадцати лет	К допускаемой к обороту информационной продукции для детей, достигших возраста шестнадцати лет, может быть отнесена информационная продукция, предусмотренная статьей 9 настоящего Федерального закона, а также информационная продукция, содержащая оправданные её жанром и (или) сюжетом: 1) изображение или описание несчастного случая, аварии, катастрофы, заболевания, смерти без натуралистического показа их последствий, которые могут вызывать у детей страх, ужас или панику; 2) изображение или описание жестокости и (или) насилия (за исключением сексуального насилия) без натуралистического показа процесса лишения жизни или нанесения увечий при условии, что выражается сострадание к жертве и (или) отрицательное, осуждающее отношение к жестокости, насилию (за исключением насилия, применяемого в случаях защиты прав граждан и охраняемых законом интересов общества или государства); 3) информация о наркотических средствах или о психотропных и (или) об одурманивающих веществах (без их демонстрации), об опасных последствиях их потребления с демонстрацией таких случаев при условии, что выражается отрицательное или осуждающее отношение к потреблению таких средств или веществ и содержится указание на опасность их потребления; 4) отдельные бранные слова и (или) выражения, не относящиеся к нецензурной брани; 5) не эксплуатирующие интереса к сексу и не носящие оскорбительного характера изображение или описание половых отношений между мужчиной и женщиной, за исключением изображения или описания действий сексуального характера
Источник: http://www.consultant.ru		

Статья 14. Федерального закона «О защите детей от информации, причиняющей вред их здоровью и развитию» раскрывает особенности распространения информации посредством информационно-телекоммуникационных сетей:

1. Доступ к информации, распространяемой посредством информационно-телекоммуникационных сетей, в том числе сети Интернет, в местах, доступных для детей, предоставляется лицом, организующим доступ к сети Интернет в таких местах (за исключением операторов связи, оказывающих эти услуги связи на основании договоров об оказании услуг связи, заключенных в письменной форме), другим лицам при условии применения административных и организационных мер, технических, программно-аппаратных средств защиты детей от информации, причиняющей вред их здоровью и (или) развитию.

2. Сайт в информационно-телекоммуникационной сети Интернет, не зарегистрированный как средство массовой информации, может содержать знак информационной продукции (в том числе в машиночитаемом виде) и (или) текстовое предупреждение об ограничении её распространения среди детей, соответствующие одной из категорий информационной продукции, установленных частью 3 статьи 6 настоящего Федерального закона. Классификация сайтов осуществляется их владельцами самостоятельно в соответствии с требованиями настоящего Федерального закона.

3. Аудиовизуальный сервис должен содержать знак информационной продукции (в том числе в машиночитаемом виде) и (или) текстовое предупреждение об ограничении распространения среди детей информационной продукции, соответствующие одной из категорий информационной продукции, установленных частью 3 статьи 6 настоящего Федерального закона. Классификация аудиовизуальных сервисов осуществляется их владельцами самостоятельно в соответствии с требованиями настоящего Федерального закона (часть 3 введена Федеральным законом от 01.05.2017 № 87-ФЗ).

Экспертиза информационной продукции проводится экспертом, экспертами и (или) экспертными организациями, аккредитованными уполномоченным Правительством Российской Федерации федеральным органом исполнительной власти, по инициативе органов государственной власти, органов местного самоуправления, юридических лиц, индивидуальных предпринимателей, общественных объединений, граждан на договорной основе (Ст.17. Федерального закона «О защите детей от информации, причиняющей вред их здоровью и развитию» раскрывает особенности распространения информации посредством информационно-телекоммуникационных сетей»).

1 сентября 2012 года вступил в силу Федеральный закон «О внесении изменений в отдельные законодательные акты Российской Федерации в

связи с принятием Федерального закона «О защите детей от информации, причиняющей вред их здоровью и развитию» от 21.07.2011 № 252-ФЗ.

В 2015 году была разработана Концепция информационной безопасности детей (распоряжения Правительства РФ от 02.12.2015 № 2471-р «Об утверждении Концепции информационной безопасности детей»). В ней определены основные принципы обеспечения информационной безопасности детей, приоритетные задачи и механизмы реализации госполитики в этой области, ожидаемые результаты.

В основу положено признание детей равноправными участниками процесса формирования информационного общества. Закреплено, что обеспечение информационной безопасности детей возможно исключительно при условии эффективного сочетания государственных и общественных усилий при определяющей роли семьи.

Среди приоритетных задач госполитики в этой сфере названы формирование у детей навыков самостоятельного и ответственного потребления информационной продукции, повышение уровня медиаграмотности детей, воспитание у детей уважительного отношения к интеллектуальной собственности и авторскому праву, сознательный отказ от использования «пиратского» контента.

Наиболее эффективным способом регулирования информационного потребления с целью обеспечения безопасности детей признан вариант сорегулирования медиасообществом и государством.

Отмечено, что усилия государства по ограничению доступа к ресурсам, содержащим противоправный контент, не могут полностью оградить детей от вредной информации. Поэтому необходимо формировать у детей механизмы критической оценки получаемых сведений.

Совместные усилия семьи, общества и государства следует направить на то, чтобы ребёнок с детства привыкал свободно ориентироваться в медиапространстве, умел взаимодействовать с различными источниками информации, не поддавался манипуляциям извне и мог делать самостоятельные выводы о качестве информационных продуктов (https://www.garant.ru).

Ожидаемым результатами от её реализации к 2020 году называлось формирование в Российской Федерации поколения молодых граждан, которые смогут свободно и самостоятельно ориентироваться в современном информационном пространстве. Для этого необходимо следующее:

- *наличие развитых информационно-коммуникационных механизмов, направленных на социализацию молодого поколения и раскрытие его творческого потенциала;*
- *свободный доступ детей к историко-культурному наследию предшествующих поколений;*
- *качественный рост уровня медиаграмотности детей;*
- *увеличение числа детей, разделяющих ценности патриотизма;*

- *гармонизация меж- и внутрипоколенческих отношений;*
- *популяризация здорового образа жизни среди молодого поколения;*
- *формирование среди детей устойчивого спроса на получение высококачественных информационных продуктов;*
- *снижение уровня противоправного и преступного поведения среди детей;*
- *формирование у детей уважительного отношения к интеллектуальной собственности и авторскому праву, сознательный отказ от использования «пиратского» контента.*

В настоящее время по-прежнему актуальна работа по заданному в Концепции направлению создания медиасреды, соответствующей названным характеристикам.

Для обеспечения информационной безопасности в образовательной организации, администрации ОО необходимо руководствоваться документом «Правила подключения общеобразовательных учреждений к единой системе контент-фильтрации доступа к сети Интернет, реализованной Министерством образования и науки Российской Федерации», утвержденным министром образования и науки Российской Федерации А.А. Фурсенко 11 мая 2011 года (№ АФ-12/07вн).

2. Обеспечение информационной безопасности детей и подростков

Медиа – это обширное понятие, которое включает в себя всю совокупность средств и приемов, служащих для передачи информации человеку. Это могут быть:

✓ *медиасредства массовой информации* (телевидение, периодическая пресса, радио, кабельные телевизионные сети);

✓ *директ медиа* – коммуникационные системы передачи информации (интернет, телефон, почта);

✓ *медианосители* – отдельные носители информации (письма, записи на аудио- и видеоносителях, видео-, аудио-, презентации);

✓ *социальные медиа* – средства коммуникации групп сообществ между собой (социальные сети, блоги, персональные сайты, самиздатовская периодическая пресса).

Безопасность – это состояние защищённости жизненно важных интересов личности, общества, государства от внутренних и внешних угроз.

Информационная безопасность детей – состояние защищенности детей, при котором отсутствует риск, связанный с причинением информацией вреда их здоровью и (или) физическому, психическому, духовному, нравственному развитию. Информационная безопасность также может быть обозначена как практика предотвращения несанкционированного доступа,

использования, раскрытия, искажения, изменения, исследования, записи или уничтожения информации. На сайтах, предназначенных для защиты пользователей, в открытом доступе содержится информация, которую необходимо знать не только педагогам образовательной организации, но и родителям и, конечно, обучающимся.

Рассмотрим основные понятия.

Цифровой след, иногда называемый цифровой тенью или электронным следом – это данные, которые пользователь оставляет при использовании интернета. Эти данные включают посещаемые веб-сайты, отправляемые электронные письма и информацию, указываемую в онлайн-формах. Цифровой след можно использовать для отслеживания действий человека и его устройств в интернете. Пользователи интернета активно или пассивно создают собственный цифровой след. Расширению цифрового следа способствуют публикации в социальных сетях, подписки на информационные рассылки, оставленные отзывы и покупки в интернете. Процесс расширения цифрового следа не всегда очевиден, например, веб-сайты могут отслеживать активность, устанавливая файлы cookie на устройство, а приложения могут считывать данные без ведома пользователя. Применительно к цифровым следам часто используются термины «активный» и «пассивный».

Активный цифровой след.

Пользователь оставляет активный цифровой след, когда намеренно делится информацией о себе: делает публикации в социальных сетях или оставляет сообщения на сайтах или онлайн-форумах. Если пользователь вошел на веб-сайт с использованием зарегистрированного имени или профиля, все опубликованные им сообщения будут составлять его активный цифровой след. Также активный цифровой след остается при заполнении онлайн-форм, например, подписке на информационные рассылки или при согласии принимать файлы cookie в браузере.

Пассивный цифровой след.

Пассивный цифровой след создается, когда информация о пользователе собирается без его ведома. Это происходит, например, когда на веб-сайте собирается информация о том, сколько раз пользователи посещали сайт, откуда эти пользователи и их IP-адреса. Это скрытый процесс, о котором пользователи могут не догадываться. Другим примером использования пассивного следа является анализ рекламодателями лайков, репостов и комментариев в социальных сетях с целью последующего профилирования и отображения вам определенного контента.

Цифровые следы важны по следующим причинам:

Они относительно постоянны. Как только информация становятся общедоступной (полностью или частично).

Цифровой след может отражать цифровую репутацию человека, которая теперь считается такой же важной, как и репутация за пределами сети.

Прежде чем принимать решения о найме, работодатели могут проверять цифровые следы своих потенциальных сотрудников, особенно их социальные сети. Колледжи и университеты могут проверять цифровые следы своих будущих студентов перед зачислением на учебу.

Публикуемые в интернете сообщения и фотографии могут быть неверно истолкованы или изменены, что может привести к непреднамеренному оскорблению.

Контент, предназначенный для узкой группы, может распространиться на более широкий круг и испортить отношения и дружбу.

Киберпреступники могут использовать цифровой след в целях фишинга, для доступа к учетной записи или для создания ложных профилей на основе данных пользователя (фи́шинг (англ. phishing от fishing «рыбная ловля, выуживание» – вид интернет-мошенничества, целью которого является получение доступа к конфиденциальным данным пользователей – логинам и паролям).

Цифровой след пользователя интернета может включать сотни составляющих. Вот лишь некоторые действия, увеличивающие цифровой след: *онлайн-покупки, интернет-банкинг, социальные медиа, чтение новостей, приложения «здоровье и фитнесс»* и т.д.

Многие пытаются управлять своим цифровым следом, с осторожностью выполняя действия в сети и в первую очередь контролируя потенциально собираемые данные. Существуют способы защиты цифрового следа.

Поскольку работодатели, университеты и другие лица могут проверить ваши данные в интернете, рекомендуется с внимательностью относиться к цифровому следу. Это касается не только взрослых, но и детей и подростков. Ниже приведены несколько рекомендаций по защите личных данных и управлению репутацией в сети (Таблица 2).

Таблица 2

Способы защиты цифрового следа

Способ защиты	Действия
Использование поисковых систем для проверки своего цифрового следа	Введите свое имя в поисковую систему. Укажите имя и фамилию, используйте все варианты написания. Если вы меняли имя, выполните поиск как текущего, так и прежнего имени. Просмотр результатов поиска даст вам представление об общедоступной информации о вас. Если какой-либо из результатов поиска показывает вас не в лучшем свете, можно связаться с администраторами сайта и узнать, могут ли они удалить эту информацию

Уменьшение количества источников информации, в которых упоминается ваше имя	Например, веб-сайты, посвященные недвижимости могут содержать о вас больше информации, чем хотелось бы. Эти сайты могут содержать личную информацию: номер телефона, адрес и возраст. Если вас это не устраивает, можно связаться с администраторами веб-сайтов и запросить удаление информации
Ограничение объема предоставляемых данных	Каждый раз при предоставлении личной информации вы расширяете свой цифровой след, а также увеличиваете вероятность того, что компания, хранящая ваши данные, воспользуется ими не по назначению или подвергнется взлому, в результате чего ваши данные могут попасть злоумышленникам. Поэтому прежде чем заполнять форму, подумайте, стоит ли это делать. Есть ли другие способы получить информацию или услугу без предоставления личных данных?
Проверка параметров конфиденциальности	Параметры конфиденциальности в социальных сетях позволяют контролировать, кто видит ваши публикации. Проверьте, настроены ли эти параметры на комфортном для вас уровне. Многие ресурсы позволяют ограничивать видимость публикаций для друзей и создавать специальные списки тех, кто может видеть определенные публикации. Однако не забывайте, что параметры конфиденциальности защищают вас только в конкретной социальной сети
Избегание раскрытия излишней информации в социальных сетях	Социальные сети позволяют легко общаться с людьми, однако провоцируют на раскрытие излишней информации. Подумайте, стоит ли указывать свое местоположение, раскрывать планы поездок или другую личную информацию. Не указывайте номер телефона и адрес электронной почты в разделе «Информация» в социальных сетях. Также не рекомендуется ставить лайки вашему банку, компании, предоставляющей медицинские услуги, аптеке и прочим организациям, поскольку это может указать киберпреступникам на ваши важные учетные записи
Избегание незащищенных веб-сайтов	Убедитесь, что вы совершаете транзакции на защищенном веб-сайте. Его веб-адрес должен начинаться с **https://,** а не с **http://;** буква s означает «безопасный» и указывает на наличие у сайта сертификата безопасности. Слева от адресной строки также дол-

	жен отображаться значок замка. Не разглашайте конфиденциальную информацию, особенно платежные данные, на незащищенных сайтах
Защита личных данных при использовании публичных сетей Wi-Fi	Публичная сеть Wi-Fi менее безопасна, чем ваша личная сеть: неизвестно, кто её настраивал и кто может иметь к ней доступ. Избегайте предоставления личной информации при использовании публичных сетей Wi-Fi
Удаление старых учетных записей	Один из способов уменьшить свой цифровой след – удалить старые учетные записи, например, неиспользуемые профили в социальных сетях и подписки на не интересующие вас информационные рассылки. Удаление неиспользуемых учетных записей снижает вероятность утечки данных
Создание надежных паролей и использование менеджер паролей	*Надежный пароль* помогает обеспечить безопасность в интернете. Надежный пароль является длинным – состоит не менее чем из 12 символов, а в идеале больше, и содержит сочетание заглавных и строчных букв, символов и цифр. Чем сложнее ваш пароль, тем сложнее его взломать. Использование *менеджера паролей* позволяет создавать, хранить и управлять всеми паролями с помощью единой защищенной учетной записи. Пароли необходимо хранить в секрете, никому не сообщать и нигде не записывать. Рекомендуется не использовать один пароль для всех учетных записей, а также регулярно менять пароли
Сохранение конфиденциальности медицинских документов	Соблюдайте правила защиты данных и регулярно проверяйте свои медицинские документы. Похитители личных данных нацелены на медицинскую и финансовую информацию. Если преступники используют вашу личную информацию для получения медицинских услуг от вашего имени, их медицинские документы могут объединиться с вашими
Поддержание актуальности программного обеспечения	Устаревшее программное обеспечение может содержать множество цифровых следов. Если не установить последние обновления, киберпреступники могут получить доступ к этой информации. Используя уязвимости в программном обеспечении, они могут с легкостью получить доступ к устройствам и данным. Регулярное обновление программного обеспечения позволяет предотвратить это, поскольку устаревшее программное обеспечение является более уязвимым для атак злоумышленников

Настройка использования мобильного устройства	Установите пароль для мобильного устройства, чтобы в случае утери никто, кроме вас, не мог получить к нему доступ. При установке приложений ознакомьтесь с пользовательским соглашением. Для многих приложений в нем описано, какую информацию оно собирает и для чего она может использоваться. Приложения могут собирать личные данные, такие как электронная почта, местоположение и действия в интернете. Прежде чем использовать приложение, убедитесь, что вас устраивает, какую информацию оно собирает
Оценка материалов перед публикацией	На основе ваших публикаций и комментариев в интернете, а также по отзывам других людей формируется мнение о вас. Некоторые аспекты вашего цифрового следа, например, загруженные фотографии, комментарии в блогах, видео и публикации, могут показать вас совсем не с той стороны, с которой вы бы хотели. Создавайте положительный цифровой след, публикуя только то, что создает вам желаемый образ
Принятие немедленных мер в случае взлома	Если вы предполагаете, что ваши данные могли быть скомпрометированы в результате взлома, немедленно примите меры. Если речь идет о финансовых потерях, сообщите о нарушении в банк или компанию, выпустившую кредитную карту. Измените все пароли, которые могли быть раскрыты. Если скомпрометированный пароль использовался для других учетных записей, измените его везде
Источник: https://www.kaspersky.ru	

Интернет-безопасность – это безопасность действий и транзакций, совершаемых в интернете. Интернет-безопасность входит в более широкие понятия, такие как кибербезопасность и компьютерная безопасность, и включает безопасность браузера и сети, а также правильное поведение в сети. Проводя значительное время в сети, можно столкнуться со следующими угрозами интернет-безопасности:

Взлом – получение неавторизованными пользователями доступа к компьютерным системам, учетным записям электронной почты и веб-сайтам.

Вирусы и вредоносные программы, которые могут повредить данные и сделать системы уязвимыми для других угроз.

Кража личных данных, например, личной и финансовой информации злоумышленниками.

Таблица 3

Распространенные угрозы интернет-безопасности

Угроза интернет-безопасности	Определение понятия
Фишинг	Это кибератака с использованием поддельных писем. Злоумышленники пытаются обмануть получателей электронной почты, убедив их в подлинности и актуальности сообщения. Например, они маскируют письма под запросы из банка или сообщения от коллег, чтобы пользователи переходили по ссылкам или открывали вложения. Цель атаки состоит в том, чтобы обманным путем заставить пользователей раскрыть личную информацию или загрузить вредоносные программы
Взлом и удаленный доступ	Злоумышленники всегда стремятся использовать уязвимости частной сети или системы для кражи конфиденциальной информации и данных. Технология удаленного доступа предоставляет им дополнительные возможности. Программное обеспечение для удаленного доступа позволяет пользователям получать доступ к компьютеру и управлять им удаленно. Его использование значительно выросло в период пандемии, когда все больше людей работают удаленно
Вредоносные программы и вредоносная реклама	Термин вредоносные программы охватывает все программы: вирусы, черви, трояны и прочие, которые злоумышленники используют для нанесения ущерба и кражи конфиденциальной информации. Любое программное обеспечение, предназначенное для повреждения компьютера, сервера или сети, может расцениваться как вредоносное. Термин «вредоносная реклама» описывает онлайн-рекламу, распространяющую вредоносные программы. Пользователи, взаимодействующие с вредоносной рекламой, могут загрузить вредоносные программы на свое устройство или перейти на вредоносные веб-сайты
Программы-вымогатели	Программы-вымогатели – это вредоносные программы, блокирующие использование компьютера или доступ к определенным файлам на компьютере, пока не будет уплачен выкуп. Они часто распространяются как троянские программы – вредоносные программы, замаскированные под легальные. После установки программа-вымогатель блокирует экран системы или определенные

	файлы до тех пор, пока злоумышленники не получат выкуп
Ботнеты	Термин ботнет означает сеть компьютеров, специально зараженных вредоносным ПО с целью выполнения автоматических задач в интернете без разрешения и ведома владельцев этих компьютеров. Когда компьютер управляется ботнетом, он может использоваться для выполнения злонамеренных действий, например: создание фальшивого интернет-трафика на сторонних веб-сайтах с целью получения прибыли, рассылка спама миллионам пользователей интернета, совершение мошеннических действий и кража личных данных, атаки на компьютеры и серверы. Компьютеры становятся частью ботнета так же, как и заражаются любой другой вредоносной программой: например, при открытии вложений электронной почты, загрузке вредоносных программ, посещении веб-сайтов, зараженных вредоносными программами
Опасности в публичных и домашних сетях Wi-Fi	
Использование публичных сетей Wi-Fi – в кафе, торговых центрах, аэропортах, отелях и ресторанах – сопряжено с определенными рисками, поскольку уровень безопасности в этих сетях часто низкий или защита полностью отсутствует. Это означает, что киберпреступники могут отслеживать действия пользователей в интернете и красть пароли и личную информацию	
Прослушивание сети	Злоумышленники отслеживают и перехватывают незашифрованные данные при передаче по незащищенной сети
Атаки типа «человек посередине»	Злоумышленники взламывают точку доступа Wi-Fi и подключаются к процессу передачи данных между пользователем и точкой доступа с целью перехвата и изменения данных в процессе передачи
Мошеннические сети Wi-Fi	Злоумышленники создают приманку в виде бесплатной сети Wi-Fi для сбора личных данных. Точка доступа злоумышленника служит каналом для всех данных, передаваемых по сети
Источник: https://www.kaspersky.ru	

Существует множество опасностей, подстерегающих ребёнка в Интернет-пространстве. Необходимо знать о них и о способах защиты (таблица 3 «Распространенные угрозы интернет-безопасности» и таблица 4 «Обеспечению безопасности детей в интернете»).

Есть возможности защититься от подобных угроз, используя приёмы интернет-безопасности (таблица 4).

Таблица 4

Защита личных данных в сети

Способ защиты	Действия
Тщательный выбор браузера	Браузер – это основной инструмент для выхода в интернет, он играет ключевую роль в обеспечении безопасности в интернете. Хороший веб-браузер должен быть безопасным и обеспечивать защиту от утечки данных. Фонд свободы прессы составил подробное руководство, описывающее плюсы и минусы безопасности основных веб-браузеров
Использование сетевого экрана	Сетевой экран исполняет роль барьера между вашим компьютером и сетью, например интернетом. Сетевые экраны блокируют нежелательный трафик, а также помогают предотвратить заражение компьютера вредоносными программами. Часто сетевой экран входит в состав операционной системы или системы безопасности. Для обеспечения максимальной безопасности в интернете рекомендуется убедиться, что сетевой экран включен и настроено автоматическое обновление
Создание надежных паролей и использование менеджера паролей	Надежный пароль помогает обеспечить безопасность в интернете. Пароли необходимо хранить в секрете, никому не сообщать и нигде не записывать. Рекомендуется не использовать один пароль для всех учетных записей, а также регулярно менять пароли
Использование на устройствах последней версии программы безопасности	Антивирус, обеспечивающий защиту в интернете, очень важен для сохранения конфиденциальности и безопасности. Лучшие программы интернет-безопасности защищают от различных видов атак, а также обеспечивают безопасность данных в интернете. Очень важно обновлять антивирусное программное обеспечение. Большинство современных программ обновляются автоматически, что гарантирует защиту от последних угроз интернет-безопасности
Защита электронной почты *Безопасность электронной почты – это набор методов, используемых для защиты учетных записей электронной почты и переписки от несанкционированного доступа, потери и компрометации. Учитывая, что электронная почта часто используется для распространения вредоносных программ, спама и фишинговых атак, её безопасность является важным аспектом безопасности в интернете.*	

Слишком много спам-писем может быть признаком того, что ваш адрес электронной почты был раскрыт в результате утечки данных. В этом случае рекомендуется сменить адрес электронной почты	
Отмечать спам-сообщения как спам	Способ отметить сообщение как спам зависит от используемого почтового клиента: Outlook, mail, и т. д.
Никогда не переходить по ссылкам и не открывать вложения в спам-сообщениях	В результате таких действий на устройство могут быть загружены вредоносные программы. По крайней мере, такие действия служат подтверждением для спамеров, что это активная учетная запись электронной почты, и стимулируют их рассылать еще больше спама
Соблюдать осторожность при использовании адреса электронной почты	Полезно иметь дополнительную временную учетную запись электронной почты, используемую исключительно для регистрации и подписки. Она должна отличаться от рабочей и от используемой для переписки с друзьями и близкими
Настройки конфиденциальности провайдеров	Большинство провайдеров электронной почты имеют настройки конфиденциальности. Убедитесь, что они установлены на комфортном для вас уровне
Изучить сторонние спам-фильтры для электронной почты	Они обеспечивают дополнительный уровень кибербезопасности, поскольку электронные письма, прежде чем попасть к адресату, должны пройти через два спам-фильтра: спам-фильтр почтового провайдера и сторонний фильтр
Источник: https://www.kaspersky.ru	

Защита детей от опасного и неприемлемого контента и контактов в интернете, а также от вредоносных программ и атак очень важна. Обучение детей основам безопасности в Интернете позволит их обезопасить.

Дети проводят все больше и больше времени в интернете, и важно объяснить им, как оставаться в безопасности. Важно, чтобы они знали, какую информацию следует хранить в секрете. Например, следует объяснить, почему никому нельзя сообщать пароли и раскрывать личную информацию. Установка компьютера там, где вы можете наблюдать и контролировать его использование, также поможет обеспечить безопасность ребёнка в интернете.

Существует набор настроек «Родительский контроль», позволяющий контролировать контент, доступный ребёнку в интернете. Родительский контроль, используемый совместно с настройками конфиденциальности, повышает безопасность детей в интернете. Настройка родительского контроля зависит от платформы и устройства. Можно также использовать различные приложения для родительского контроля, например, Kaspersky Safe Kids.

3. Психологическая безопасность в цифровом пространстве

Психологическую безопасность определяют как переживание личностью психологического комфорта, выражающееся в осознании собственного статуса, чувства собственного достоинства и их неприкосновенности, а также в эмоциональном принятии себя. В аспекте взаимодействия личности со средствами массовой информации (СМИ) психологическая безопасность означает невмешательство СМИ в личностное пространство человека.

Информационно-психологическая безопасность – это эффективное использование имеющихся информационных ресурсов с целью необходимости обеспечения защиты общества, отдельных его групп и личности от негативного воздействия деструктивных видов и форм информации; обеспечения защиты в первую очередь детей и несовершеннолетних членов общества от тех видов информации, которые представляют опасность для их жизни и здоровья либо могут нанести вред их нравственному, духовному, психическому, физическому и социальному развитию. В образовательной организации для создания психологически безопасной среды необходимо участие всех участников образовательного процесса.

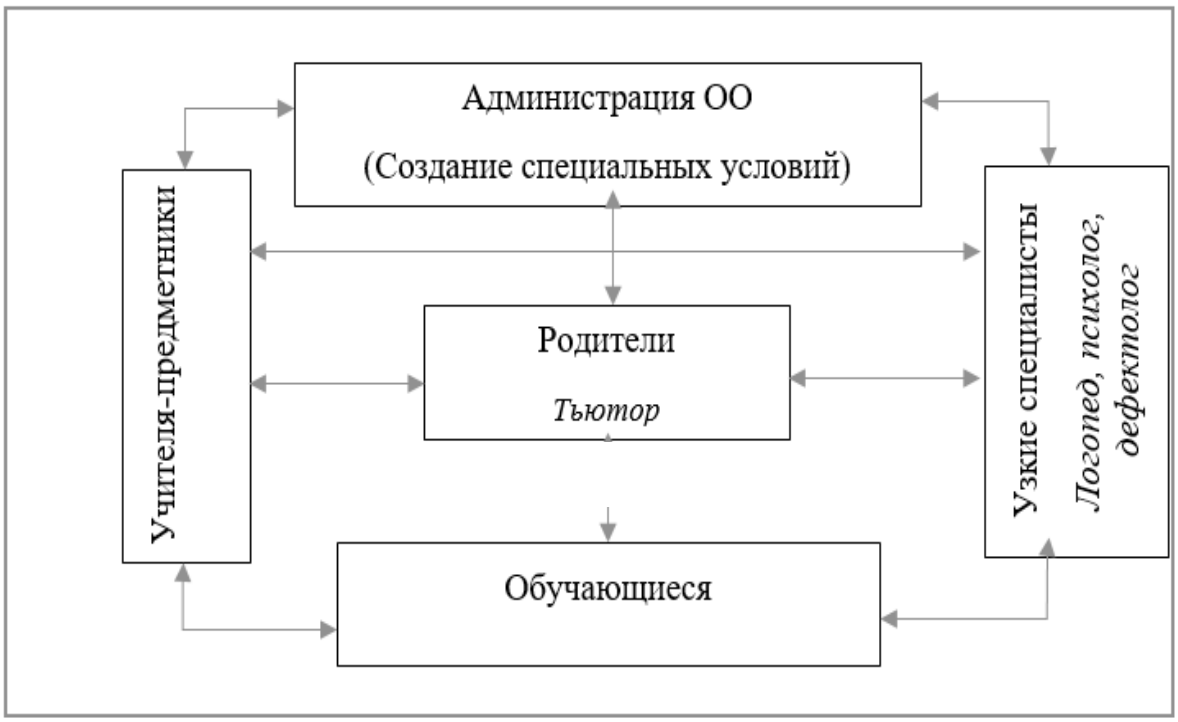

Рис. 1. *Примерная схема взаимодействия участников образовательного процесса для создания психологической безопасности в ОО*

К сожалению, не всегда удается полностью контролировать среду, в которой обучающиеся находят свои интересы, общаются и знакомятся с людьми. Общение в сети может быть не только полезным и интересным, но и опасным и непредсказуемым.

Достаточно распространенным явлением в подростковой среде является интернет-травля, или кибертравля (кибербуллинг) – намеренные оскорбления, буллинг, угрозы, диффамации и сообщение другим компрометирующих данных с помощью современных средств коммуникации, как правило, в течение продолжительного периода времени.

Распространение кибербуллинга в последние годы вызывает беспокойство во всем мире, ставя под угрозу безопасность подростков, пользующихся Интернетом. Известно, что не только подростки-жертвы имеют психологические и поведенческие проблемы, но и подростки-агрессоры также страдают от последствий данного феномена и подвергаются риску поведенческих девиаций и нарушения психического здоровья.

В.Н. Бородина и А.И. Петимко (2021) описывают механизм реализации кибербуллинга через различные действия агрессора в интернет-пространстве, начиная от распространения слухов, недостоверной информации о человеке, обидных комментариев, повторяющихся оскорбительных сообщений, сообщений-угроз, в том числе членам семьи, исключения из сообществ, кражи персональных данных и их распространение в сети, интенсивного эмоционального обмена репликами с вовлечением большого количества людей до распространения конфиденциальной информации, интимных фотографий другого человека без его разрешения. Для осуществления данных негативных действий используются электронная почта, чаты, сайты социальных сетей, веб-страницы, фотографии, видеоматериалы, онлайн-игры и т.д.

В знаменитой книге Пэтчин Д., Хиндуя С. «Написанное остается. Как сделать интернет-общение безопасным и комфортным» авторы отмечают, что кибербуллинг оказывает негативное воздействие и на жертву, например, снижает самооценку, усиливает депрессию и вызывает чувство бессилия. Те учащиеся, которые подвергались онлайн-издевательствам, переживали разочарование, гнев, обиду, тревогу, социальную изоляцию. В своем исследовании авторы указывают на связь между травлей в сети и низкой самооценкой, семейными проблемами, снижением успеваемости, насилием в школе и различными видами преступного поведения, причем проблемы имеют не только подростки-жертвы, но и подростки-агрессоры. Более 60% учащихся, подвергшихся кибербуллингу, сообщили, что это негативное явление сильно повлияло на их способность учиться и чувствовать себя в безопасности в школе. Учащиеся средних и старших классов, подвергавшиеся школьным или онлайн-издевательствам, значительно чаще сообщали о суицидальных мыслях, намерениях. При этом исследователями отмечается, что виктимизация кибербуллинга была более тесно связана с суицидальными мыслями и поведением, чем виктимизация школьных издевательств.

Помимо кибербуллинга существуют и другие риски возникновения деструктивного поведения у детей и подростков, возникающие под воздействием распространяемой в сети Интернет информации.

Специалисты АНО «Центр изучения и сетевого мониторинга молодежной среды» и ФГБУ «Центр защиты прав и интересов детей» в 2020 году опубликовали алгоритмы действий для педагогов и родителей по раннему выявлению и реагированию на деструктивное поведение несовершеннолетних, проявляющееся под воздействием информации негативного характера, распространяемой в сети Интернет. Авторы определяют деструктивное поведение как форму активности личности, связанную с разрушением субъектом структур, как «составляющих» его (организм), так и заключающих его в «себе» (общество). В зависимости от определенных ситуационных, социокультурных и индивидуально-психологических факторов деструкция может быть направлена человеком на самого себя или вовне, выступать в виде импульсивного, неосознанного, рефлекторного или сознательного, расчетливого поступка. Профилактика деструктивного поведения основана на социализации несовершеннолетних, формировании у них нравственных качеств субъектов социальных отношений. Институтом социализации детей является семья и школьная среда, где закладываются идеалы и базисы, из которых формируется дальнейшее мировоззрение, морально-этические ориентиры и общая направленность поведения.

Одним из ключевых моментов, описанных в алгоритме действий по раннему выявлению и реагированию на деструктивное поведение несовершеннолетних, проявляющееся под воздействием информации негативного характера, распространяемой в сети Интернет, является понимание основных опасностей в сети Интернет для детей и подростков и умение распознавать признаки вовлечения детей в деструктивные отношения и/или сообщества (таблицы 5, 6).

Таблица 5

Основные опасности в сети интернет для детей и подростков

Риски	Информация о рисках	Примечания
Коммуникационные риски	**Кибербуллинг** (интернет-травля, преследование сообщениями, содержащими оскорбления, агрессию, запугивание; хулиганство); **Социальное бойкотирование** с помощью различных интернет- сервисов; публикация и рассылка контента интимного характера	**Меры помощи ребёнку, подвергшемуся кибербуллингу:** • психологическая поддержка педагогом и родителями; • изменение настроек приватности профиля подростка в соцсетях (убрать личную информацию, закрыть аккаунт от посторонних людей); • создание новой учетной записи для ребёнка с измененным именем и фотографией профиля, чтобы обидчик не смог продолжить травлю; • обучение правилам безопасного поведения в сети Интернет
	Деструктивные группы: использование сети Интернет для вовлечения несовершеннолетних в совершение действий, представляющих опасность для их жизни и здоровья (суицидальные сайты; форумы потенциальных самоубийц; сайты, вовлекающие в участие в опасных играх; наркосайты; сайты, разжигающие национальную рознь и расовое неприятие (экстремизм, национализм, фашизм); сайты, пропагандирующие экстремизм, насилие и девиантные формы поведения, секты)	**Этапы вовлечения несовершеннолетних в деструктивные группы:** • предоставление ложной информации (соответствующий тематический материал в сети, фото-, видеоинформация); • общение, взаимодействие с вербовщиком сети; • исполнение подростком указанных вербовщиком действий; • попадание в зависимость

	«Незнакомый друг» в социальных сетях (прямые угрозы жизни и здоровью от незнакомцев, предлагающих личные встречи)	**ВАЖНО!** **ОБУЧЕНИЕ ПРАВИЛАМ БЕЗОПАСНОГО ПОВЕДЕНИЯ В СЕТИ ИНТЕРНЕТ**
	Груминг (установление дружеского и эмоционального контакта с ребёнком в сети Интернет для его дальнейшей сексуальной эксплуатации)	
	Кибersталкинг (преследование ребёнка переходит из виртуального мира в реальный)	
Контентные риски	**«Шок-контент» (**материалы (тексты, фото, видео, аудио), которые законодательно запрещены для публикации, вызывают у пользователя резко негативные чувства и ощущения: страх, ужас, отвращение, унижение)	**ВАЖНО!** **ИСПОЛЬЗОВАТЬ ПРИЛОЖЕНИЯ ДЛЯ РОДИТЕЛЬСКОГО КОНТРОЛЯ**
	Просмотр сайтов для взрослых	
Технические риски	**Незаконный сбор персональных данных** несовершеннолетних и (или) распространение их в открытом доступе; **Повреждение** устройств, программного обеспечения	**ВАЖНО!** **ИЗУЧИТЬ И ИСПОЛЬЗОВАТЬ СПОСОБЫ ЗАЩИТЫ ЦИФРОВОГО СЛЕДА И ПЕРСОНАЛЬНЫХ ДАННЫХ**
Потребительские риски	**Кража личных данных** техническими средствами (в том числе в процессе интернет-шопинга); **Кибермошенничество**	

Таблица 6

Основные признаки изменений деструктивного поведения у обучающихся и действия педагога и родителя при их обнаружении

Психологические признаки	Изменения в поведении ребёнка	Изменения во внешнем виде	Необходимые действия педагога	Необходимые действия родителей
• Повышенная возбудимость, тревожность, перерастающая в грубость, откровенную агрессию; • зацикленность на негативных эмоциях, склонность к депрессии; • проявление навязчивых движений; • неспособность сопереживать, сочувствовать другим людям; • утрата прежнего эмоционального контакта с одноклассниками; • стремление показать свое «бесстрашие» окружающим;	• Конфликтное поведение; • ведение тетради/ записной книжки для записи имен, агрессивные высказывания в их отношении, негативные рисунки, угрозы; • проявление интереса к неприятным зрелищам, сценам насилия; • участие в поджогах, «играх» с взрывоопасными веществами; • трансляция деструктивного контента в социальных сетях, «лайки»); • навязчивое рисование (пугающие картины, заштриховывает бумагу);	• Использование деструктивной символики во внешнем виде (одежда с агрессивными надписями и изображениями); • наличие (появление) синяков, ран, царапин на теле или голове; • нежелание следить за своим внешним видом, появление следов краски на одежде, руках (в случае нанесения на поверхности рекламы интернет-магазинов наркотиков часто используются	Привлечь к работе с несовершеннолетним педагога- психолога для проведения диагностических и, при необходимости, коррекционных мероприятий. Проинформировать родителей (законных представителей) несовершеннолетнего и определить единую воспитательную стратегию, проинформировать классного руководителя. Сообщить о признаках противоправных деяний несовершен-	Проявить к ребёнку ласку и заботу, постараться открыто обсудить причины поведения, появления деструктивных признаков, но при этом не допускать в речи осуждающих фраз и не обвинять его в совершении чего-либо предосудительного. Выбрав подходящий момент, рассказать о своих проблемах и переживаниях в его возрасте, о собственном отношении к выявленной проблеме (к наркотикам, жестоко-

• стремление быть в центре внимания любой ценой; • нелюдимость, отчужденность в школьной среде; • отсутствие друзей, низкие коммуникативные навыки; • избегание зрительного контакта (уводит взгляд; • предпочитает смотреть вниз, себе под ноги)	• участие в образовании неформальных социальных групп сверстников; • жестокое обращение с животными, со сверстниками; • внезапные изменения в поведении (отказ от обучения, участия в школьных мероприятиях и т.д.); • пассивный протест (уходы из дома, отказ от еды, от общения); • подражание асоциальным формам поведения авторитетных для ребёнка людей; • появление у несовершеннолетнего (приобретение) предметов и веществ, которые могут быть использованы для закладок наркотиков (перочинные складные ножи, пластиковые пакеты малого размера;	аэрозольные баллоны); • появление у несовершеннолетнего дорогостоящей обуви, одежды, других вещей, собственных денежных средств, источник получения которых он не может объяснить (данный факт может свидетельствовать о получении дохода от наркоторговли)	нолетнего администрации образовательной организации для принятия решения об информировании сотрудника подразделения по делам несовершеннолетних органа внутренних дел	сти, травле, протестным движениям и др.). Принять меры по кратковременному изменению информационной среды несовершеннолетнего, обеспечить совместный с ним досуг в течение нескольких дней (например, без предупреждения отправиться в гости, в другой населенный пункт, на дачу, в горы или на море; внезапная пропажа ребёнка из поля зрения лица, вовлекающего в деструкцию, часто влечет прекращение дальнейшего «сотрудничества»)

	аэрозольные баллоны с краской, трафареты (для рекламы интернет- магазинов наркотиков); • использование в речи новых, нехарактерных для конкретного несовершеннолетнего выражений, слов, терминов, криминального сленга; повторяющиеся, как будто заученные, тексты			
! Единовременное наличие нескольких признаков из списка может свидетельствовать о риске участия подростка в деструктивных течениях. При проявлениях деструктивного поведения ребёнку требуется психологическая помощь				
Этапы работы педагога с несовершеннолетним обучающимся при выявлении признаков деструктивного поведения. Действия педагога при сопровождении несовершеннолетнего. Памятки для родителей и педагогов				**Приложение 1**
Пример технологической карты мероприятия, направленного на профилактику интернет-рисков в образовательной организации				**Приложение 2**

Как отмечают специалисты Центра изучения и сетевого мониторинга молодежной среды и Центра защиты прав и интересов детей, при выявлении признаков деструктивного поведения ребёнку требуется психологическая помощь. На первом этапе возможно консультирование с психологом без участия несовершеннолетнего, но если исполнение первичных рекомендаций специалиста не дает результатов, и ситуация ухудшается, то родителю необходимо посетить психолога (в образовательной организации, центре психолого-педагогической, медицинской и социальной помощи, в учреждении социального обслуживания (территориальном центре социальной помощи семье и детям, центре психолого-педагогической помощи населению, центре экстренной психологической помощи и иных), в специализированном учреждении для несовершеннолетних, нуждающихся в социальной реабилитации (социально-реабилитационном центре для несовершеннолетних и иных), в медицинской организации и иных) вместе с ребёнком, чтобы специалист смог оценить все факторы риска деструктивного поведения. Главная цель – переключить внимание и активизировать положительные качества и внутренний потенциал ребёнка, мотивировать на социально-позитивное и законопослушное поведение. Действия родителей (законных представителей) по устранению факторов риска, развитию личностных ресурсов ребёнка, созданию поддерживающей среды помогут не допустить развитие деструктивного поведения. Предупредить деструктивное поведение подростка поможет родительская забота, своевременное обращение к специалистам (психологам, медицинским работникам и др.). Всегда лучше предотвратить беду, чем исправлять разрушающий характер деструктивного поведения.

Необходимо уделять большое внимание вопросам профилактики деструктивного поведения несовершеннолетних, предупреждения негативного воздействия информации, распространяемой в сети Интернет, обеспечения сохранения жизни и здоровья детей.

Библиографический список

Нормативно-правовые источники:

1. Федеральный закон от 29 декабря 2012 г. № 273-ФЗ «Об образовании в Российской Федерации».
2. Федеральный закон от 27.07.2006 № 152-ФЗ «О персональных данных».
3. Федеральный закон от 29.12.2010 № 436-ФЗ «О защите детей от информации, причиняющей вред их здоровью и развитию».
4. Федеральный закон от 21.07.2011 № 252-ФЗ «О внесении изменений в отдельные законодательные акты Российской Федерации в связи с принятием Федерального закона "О защите детей от информации, причиняющей вред их здоровью и развитию"».
5. Федеральный закон от 27.07.2006 № 149-ФЗ «Об информации, информационных технологиях и о защите информации».
6. Федеральный закон от 28.12.2010 № 390-ФЗ (ред. от 09.11.2020) «О безопасности».
7. Распоряжение Правительства РФ от 02.12.2015 № 2471-р «Об утверждении Концепции информационной безопасности детей».

Основная литература

1. Артамонова Е.Г., Бородина А.С., Мелентьева О.С. Методические рекомендации для несовершеннолетних, родителей (законных представителей) несовершеннолетних, наглядные информационные материалы по безопасному использованию сети «Интернет» в целях предотвращения преступлений, совершаемых с её использованием, как самими несовершеннолетними, так и в отношении них: методические рекомендации. М.: ФГБУ «Центр защиты прав и интересов детей», 2021. 35 с.
2. Абрамовских Т.А. Организация медиабезопасности в образовательной организации: методические рекомендации для руководителей образовательных организаций. Челябинск: ЧИППКРО, 2018. 56 с.
3. Донцов А.И., Зинченко Ю.П., Зотова О.Ю., Перелыгина Е.Б. Психологическая безопасность личности: учебник и практикум для бакалавриата, специалитета и магистратуры. М.: Юрайт, 2019. 222 с.
4. Пэтчин Д., Хиндуя С. Написанное остается. Как сделать интернет-общение безопасным и комфортным. М.: Манн, Иванов и Фербер, 2020. 184 с.

Дополнительная литература:

1. Белоусов Е.Д. Деструктивный медиаконтент поколений Y и Z // Поколения Y и Z в постпандемийной реальности: идентификации, ориентации, поведение: сборник статей Всероссийской научно-практической конференции. Уфа, 2022. С. 17–21.

2. Бородина В.Н., Петимко А.И. Кибербуллинг среди подростков в образовательной среде как предмет исследования // Мир науки, культуры, образования. № 6 (91) 2021. С. 154–156.

3. Гринева И.Н. Эмпатия против кибербуллинга: словом можно спасти, словом можно убить // Современная журналистика в аспекте деонтологии: сборник статей. М., 2022. С. 7–14.

4. Ёркин И.Э. Нормативно-правовые документы, регламентирующие возможности для реализации медиаобразования в цифровой образовательной среде // Цифровизация общества и медиаобразовательная стратегия регионов России: сборник материалов Всероссийской научной конференции. Елец, 2021. С. 65–71.

5. Пронина, Е.Е. Матрица психологической безопасности рекламного воздействия // Информационная и психологическая безопасность в СМИ: в 2 т. Т. 1: Телевизионные и рекламные коммуникации. М., 2002. С. 292–301.

6. Кособрюхов Д.А. Медиабезопасность детей и подростков // Актуальные проблемы безопасности детей и подростков: материалы Всероссийской научно-практической конференции. Саратов, 2021. С. 192–198.

7. Чечина Т.А. На пути к медиабезопасности подрастающего поколения // Медиа–2022: теория и практика: к 150-летию МПГУ: материалы II международной научно-практической конференции / под общ. ред. Т.Н. Владимировой, В.А. Славиной, Н.В. Кодола. Москва, 2022. С. 363–367.

Электронные ресурсы

1. Сайт URL: https://www.kaspersky.ru.

2. ФГБУ «Центр защиты прав и интересов детей». URL: https://fcprc.ru.

3. Сайт Министерства просвещения Российской Федерации. URL: https://edu.gov.ru.

Приложения

Приложение 1. Этапы работы педагога с несовершеннолетними обучающимися при выявлении признаков деструктивного поведения

По материалам АНО «Центр изучения и сетевого мониторинга молодежной среды»

ФГБУ «Центр защиты прав и интересов детей», Москва, 2020 г.

1. Предварительный этап: обсуждение с педагогом-психологом и проведение диагностики подростка для определения его психофизического, педагогического, социального, психологического статуса; выявления значимых для личностного роста показателей. Составление «Карты личности подростка» и получения рекомендаций по коррекции поведения ребёнка.

2. Этап проектирования действий педагога и подростка: налаживание доверительных отношений; организация совместного с подростком поиска причин возникновения проблемы, возможных последствий её сохранения (или преодоления); взгляд на ситуацию со стороны; разделение функций и ответственности по решению проблемы; совместное определение наиболее оптимальных вариантов разрешения проблемы (конфликта, противоречия).

3. Деятельностный этап: для обеспечения успеха педагогу и педагогу-психологу важно поддержать подростка психологически; обеспечивать безопасность, защищать его интересы и права перед сверстниками, родителями, учителями. Социальный педагог может выполнять функцию развенчания негативных установок, а педагог-психолог быть «эмоциональной отдушиной» – человеком, безусловно принимающим подростка. Включение ребёнка в общественно-полезную коллективную деятельность, позволит реализовать потребность в самоутверждении.

4. Анализ результатов деятельности: совместные с подростком обсуждения успехов и неудач предыдущей деятельности, констатация факта разрешимости или неразрешимости проблемы, совместное осмысление нового опыта, определение перспектив, формирование жизненных устремлений подростка.

Действия педагога при сопровождении несовершеннолетнего

✓ Выстроить конструктивное взаимодействие с ребёнком и его родителями (законными представителями), иными значимыми для ребёнка лицами, мнение которых для него важно.

✓ Выявить проблемы, особенности развития и потенциала несовершеннолетнего.

✓ Обеспечить постоянную поддержку ребёнку в направлении позитивных изменений организовать специализированную комплексную помощь в процессе индивидуального сопровождения оказать индивидуальную помощь в развитии социальной компетентности через вовлечение подростка в различные мероприятия (учебные, воспитательные, трудовые, общественно-полезные, спортивные и др.).

✓ Обеспечить поддержку подростка социальной группой несовершеннолетних (одноклассников), имеющей позитивные социальные цели (применяется только при исключении возможности вовлечения других детей в деструктивную деятельность).

✓ Организовать взаимодействие специалистов с семьей несовершеннолетнего по его сопровождению; а также при необходимости работу по коррекции детско-родительских отношений.

Главная цель – переключить внимание и активизировать положительные качества и внутренний потенциал ребёнка, мотивировать его на социально-позитивное и законопослушное поведение.

Меры противодействия распространению деструктивных идей среди несовершеннолетних

✓ Формирование чувства неприятия насилия как такового в любом его проявлении.

✓ Формирование негативного образа и эмоционального неприятия экстремистских формирований и их лидеров.

✓ Активное развитие психологического позитивного мышления вместо разрушительного, раскрытие позитивных жизненных смыслов, развитие способности к целеполаганию.

✓ Создание комфортной социокультурной среды, микроклимата в детском коллективе, проведение политики защиты несовершеннолетних от негативного влияния Интернета, обеспечения безопасности в сети Интернет.

✓ Проведение «нравственно-правового закаливания» – формирование правовой культуры, навыков критического анализа, сопротивления негативному влиянию, развитие стойкости при неблагоприятных обстоятельствах, умения противостоять влиянию других лиц.

ПАМЯТКИ ДЛЯ РОДИТЕЛЕЙ И ПЕДАГОГОВ

По материалам ФГБУ «Центр защиты прав и интересов детей». «Как защитить ребёнка от интернет-рисков», Москва, 2018 г.

ПАМЯТКА ДЛЯ РОДИТЕЛЕЙ

Компьютерная зависимость

Компьютер становится мощным стимулом и главным объектом для общения.

На первых порах компьютер может компенсировать ребёнку дефицит общения, затем это общение может стать не нужным вовсе.

В процессе игр или нахождения в интернете ребёнок теряет контроль за временем и может проявлять агрессию в случае лишения его доступа к компьютерным играм.

Вседозволенность и простота достижения цели в играх может повлиять на уверенность ребёнка, что и в реальной жизни все так же просто и можно «заново начать» игру.

Многочасовое непрерывное нахождение перед монитором может вызвать нарушение зрения, снижение иммунитета, головные боли, усталость, бессонницу.

Могут наблюдаться проблемы с осанкой.

Дети перестают фантазировать, наблюдается эмоциональная незрелость, безответственность.

Взрослым зачастую удобно, что ребёнок занят и не отвлекает их просьбами об игре, часто такие взрослые сами зависимы от компьютера и интернета.

Подросток может пренебрегать своим внешним видом и личной гигиеной.

Могут возникать депрессии при долгом нахождении без компьютера. Могут наблюдаться проблемы с учебой.

ВАЖНО! Избавить от зависимости от компьютерных игр ребёнка нельзя, просто отобрав игрушку или запретив ему играть. Нужно не отбирать игру у зависимого от компьютерных игр, а предложить то, что будет на порядок выше, лучше, интересней.

ПАМЯТКА ДЛЯ РОДИТЕЛЕЙ

Почему дети становятся зависимыми?

Зависимость – нормальная часть жизни любого человека. Все люди зависимы от таких жизненно важных объектов, как воздух, вода, еда. Большинство людей питают здоровую привязанность к родителям, друзьям, супругам…

ВАЖНО! Когда зависимость превращается в одержимость, делает из человека раба – она становится бедой.

Виртуальная зависимость

Манипуляция человека с компьютером привела к возникновению дополнительной реальности – виртуальной,

являющейся противоположностью естественной, внешней реальности, её воображаемым, информационным эквивалентом, поскольку виртуальная реальность «имитирует» те же действия и чувства человека, которые он может испытывать в физической реальности.

ВАЖНО!

В современном мире трудно отказаться от использования информационного мирового пространства. Однако неконтролируемое использование

Интернета может таить в себе огромные опасности, особенно для подрастающего поколения, приводить к развитию особой формы психологической зависимости – «интернет-аддикции».

Термин «интернет-зависимость» был предложен Айвеном Голдбергом. Голдберг характеризует интернет-зависимость как «оказывающую пагубное воздействие на бытовую, учебную, социальную и психологическую сферы деятельности». Интернет-аддикция является новой аддикцией, качественно отличающейся от других нехимических форм выходом на безграничные возможности виртуального мира.

Компьютерная зависимость ребёнка – это хорошо видимый симптом, маркер того, что мы недостаточно знаем, что происходит с подростком, как ему живется в этом мире, каковы его проблемы и желания.

ПАМЯТКА ДЛЯ РОДИТЕЛЕЙ

РИСКИ В ИНТЕРНЕТЕ

Знакомство с новыми людьми в Интернете

Общение в Интернете может повлечь за собой коммуникационные риски, такие как незаконные контакты (например, груминг), киберпреследования, кибербуллинг и другое. Даже если у большинства пользователей добрые намерения, среди них могут быть и злоумышленники. В некоторых случаях они хотят обманом заставить детей выдать личные данные, такие как домашний адрес, телефон, пароли к персональным страницам в Интернете и другое, а могут и оказаться преступниками в поисках жертвы.

Нежелательный контент в Интернете

Контентные риски – это материалы (тексты, картинки, аудио- и видеофайлы, ссылки на сторонние ресурсы), содержащие насилие, агрессию, эротику и порнографию, нецензурную лексику, информацию, разжигающую расовую ненависть, пропаганду анорексии и булимии, суицида, азартных игр, наркотических веществ и т.д.

Сетевые компьютерные игры – это многопользовательские игры, когда одновременно играют несколько человек.

Игроки выбирают сетевые игры, где есть чат, и зачастую в нем идет не только контекстуальное общение, но и обсуждаются их проблемы, причем игроманы не игнорируют их, а, наоборот, активно включаются в их решение. Подросток, находящийся в сложной ситуации, ищет из неё выход и чаще всего – самый простой, который быстро принесет радость. Игра может стать своеобразным заменителем радости от решения проблемы, так как быстро приносит позитивные эмоции. Но это не будет её решением.

Для защиты подрастающего поколения на уровне государства разработана стратегия обеспечения информационной безопасности детей.

ВАЖНО! Только в семье могут может быть созданы условия, препятствующие развитию интернет-аддикции.

ПАМЯТКА ДЛЯ РОДИТЕЛЕЙ

Как уберечь ребёнка?

В качестве профилактики развития интернет-зависимости можно рекомендовать расширение возможностей для детей в проведении культурного, спортивного досуга, участия в общественной жизни, осуществляемых в формате межличностного эффективного общения.

Главное – самим не показывать детям примеры регулярного времяпровождения за компьютером.

Прежде чем разрешить детям работать в Интернете, рекомендуется убедиться в том, что каждый из них понимает, что можно делать в Интернете, а что нельзя.

Выработайте «семейные правила» использования Интернета. Ориентируясь на них, ребёнок будет знать, как поступать при столкновении с негативным контентом.

ВАЖНО!

Помните, что невозможно всегда находиться рядом с детьми и постоянно их контролировать. Доверительные отношения с детьми, открытый и доброжелательный диалог зачастую может быть гораздо конструктивнее, чем постоянное отслеживание посещаемых сайтов и блокировка всевозможного контента.

Для каждого ребёнка можно составить отдельный договор с правилами пользования Интернетом, установленными в соответствии с его возрастом.

Каждый ребёнок подписывает договор, подтверждая тем самым, что он понял установленные правила и согласен выполнять их при работе в Интернете.

После согласования и подписания всех пунктов семейного договора о пользовании Интернетом разместите эти договоры рядом с каждым компьютером в доме, чтобы напоминать каждому члену семьи о правилах пользования Интернетом.

ПРИМЕР

«Семейные правила» использования детьми интернета

Общие правила

1. Подключение к Сети только с разрешения родителей.

2. Нельзя открывать прикреплённые к почтовым сообщениям вложения.

3. Нельзя отвечать на обидные, недоброжелательные сообщения. О каждом таком письме надо сразу рассказать родителям.

4. Нужно быть готовым к тому, что на форумах или в чате люди не всегда те, за кого себя выдают. Даже если написано, что ресурс создан для детей – это не значит, что его не могут посещать взрослые.

5. В виртуальном пространстве, как и в реальной жизни, нужно быть вежливым и доброжелательным и покидать его, если тебя что-то раздражает.

Сетевые компьютерные игры

1. Игра не должна занимать более __-х часов на прохождение.

2. Игра не должна провоцировать на покупку виртуальных апгрейдов, без которых невозможно выиграть.

3. Игра не должна содержать сцен насилия и жестокости, а также сценариев антисоциального и преступного поведения.

4. На игру должен быть установлен согласованный с родителями лимит времени.

5. Категорически запрещается еда во время игры.

Информация

1. Дети должны сообщать родителям об опасной, неприятной и вообще любой насторожившей их информации из Интернета, от кого бы она ни исходила.

2. Нельзя доверять непроверенной информации в Интернете.

Знакомства в Интернете

1. Общаясь в сети, нельзя сообщать незнакомым людям свой телефон, адрес, номер школы, сведения о своей семье и отправлять свои фотографии.

2. Нельзя договариваться о встрече с интернет-знакомыми, не предупредив родителей.

ПРАВИЛА ДЛЯ РОДИТЕЛЕЙ ПО ИСПОЛЬЗОВАНИЮ ДЕТЬМИ ИНТЕРНЕТА

1. Старайтесь спрашивать ребёнка об увиденном в Интернете. Чаще беседуйте с ним о том, что он делает в Сети. Зачастую, открыв один сайт, ребёнок захочет познакомиться и с другими подобными ресурсами.

2. Включите программы родительского контроля и безопасного поиска, которые помогут оградить ребёнка от нежелательного контента.

3. Постоянно объясняйте ребёнку правила безопасности в Сети.

Можно даже заключить с ребёнком письменный договор.

Договор о правилах работы в Интернете

Я, _____ обязуюсь:

1. Обсудить со своими родителями правила пользования Интернетом (веб-узлы, которые я могу посещать, мои действия при использовании Интернета, время использования Интернета).

2. Никогда не сообщать свои личные данные, такие как домашний адрес, номер телефона, место работы или рабочий номер телефона моих родителей, номера кредитных карт, название или местоположение моей школы, без разрешения родителей.

3. Всегда немедленно сообщать родителям, если я увижу или получу в Интернете что-либо, что меня смутит или напугает, включая сообщения электронной почты, веб-узлы или даже обычную почту от моих интернет-друзей.

4. Никогда не соглашаться на личную встречу ни с кем из людей, с которыми я познакомился в Интернете, без разрешения родителей.

5. Никогда не отправлять свои фотографии или фотографии членов моей семьи другим людям по Интернету или по обычной почте без согласия родителей.

6. Никогда не сообщать мои интернет-пароли никому, кроме родителей (даже лучшим друзьям).

7. Не совершать в Интернете действий, которые могут нанести вред или раздражать/провоцировать других людей, либо противоречат закону.

8. Никогда не загружать, не устанавливать и не копировать ничего с дисков или из Интернета без соответствующего разрешения.

9. Никогда не совершать в Интернете действий, которые требуют оплаты, не получив сначала разрешение от родителей.

10. Разрешить родителям знать мои логины и пароли для входа на веб-узлы, а также псевдонимы для общения в Интернете, приведенные ниже …

_____
_____
_____
_____

Имя (ребёнок) _____ Дата _____

Родитель_____ Дата _____

Приложение 2. Пример технологической карты мероприятия, направленного на профилактику интернет-рисков в образовательной организации. Критерии самооценки

Критерии самооценки

Критерий	**Индикатор**
Соответствие рекомендуемой структуре технологической карты	Полное соответствие структуре
	Частичное соответствие структуре
	Несоответствие структуре
Соответствие целей и задач мероприятия индивидуальным/групповым особенностям и потребностям участников мероприятия	Полное соответствие
	Частичное соответствие
	Несоответствие
Соответствие предполагаемых результатов поставленным целям и задачам	Полное соответствие предполагаемых результатов поставленным целям и задачам; использованы предложенные инструменты
	Предполагаемые результаты в целом соответствуют поставленным целям и задачам, но не в полной мере использованы предложенные инструменты
	Есть противоречия между предполагаемыми результатами и поставленными задачами и/или целью
Соответствии форм и условий реализации мероприятия потребностям родителей	Полное соответствие
	Частичное соответствие
	Несоответствие

Примерная структура технологической карты мероприятия

ФИО педагога (организатора мероприятия) _____

Категория участников _____

Тема мероприятия _____

Тип мероприятия _____

Цель мероприятия _____

Задачи мероприятия	*Планируемые результаты

Ход мероприятия

	Название этапа мероприятия	Задача, которая должна быть решена (в рамках достижения планируемых результатов)	Формы организации деятельности участников	Действия педагога (организатора мероприятия) по организации деятельности участников	Действия участников	Результат взаимодействия участников мероприятия по достижению планируемых результатов мероприятия	Диагностика (проверка) достижения планируемых результатов
1							
…							

**Планируемые результаты указываются в соответствии с типом мероприятия, реализуемой педагогом технологии, методики*

Глоссарий

Безопасность медийная (медиабезопасность) (media safety, media protection) – способность государства, общества, социальной группы, личности обеспечить достаточные и защищенные медийные ресурсы и потоки для поддержания жизнедеятельности, устойчивого функционирования и развития соответствующего структурного образования. Обеспечение медийной безопасности предполагает противостояние негативному воздействию на индивидуальное и общественное сознание и психику людей, а также на источники информации.

Брандмауэр – это специальная программа или устройство, которое позволяет блокировать попытки хакеров, вирусов и червей получить доступ к вашему компьютеру через Интернет.

Вирусы и черви – (компьютерный вирус и компьютерный червь) – это вредоносные программы, которые способны воспроизводить себя на компьютерах или через компьютерные сети. При этом пользователь не подозревает о заражении своего компьютера. Так как каждая последующая копия вируса или компьютерного червя также способна к самовоспроизведению, заражение распространяется очень быстро. Существует очень много различных типов компьютерных вирусов и компьютерных червей, большинство которых обладают высокой способностью к разрушению.

Грамотность медийная (media literacy) (медиаграмотность) – умение анализировать и синтезировать медийную реальность, умение «читать» медиатекст, способность использовать медийную технику, знание основ медиакультуры, то есть результат медиаобразования. Аналоги – медиакомпетентность (media competence), медиакомпетенция, медийная компетентность, медийная компетенция, аудиовизуальная грамотность (audiovisual literacy).

Знак информационной продукции – графическое и (или) текстовое обозначение информационной продукции в соответствии с классификацией информационной продукции, предусмотренной частью 3 статьи 6 настоящего Федерального закона.

Информационная безопасность детей – состояние защищенности детей, при котором отсутствует риск, связанный с причинением информацией вреда их здоровью и (или) физическому, психическому, духовному, нравственному развитию.

Информационная продукция – предназначенная для оборота на территории Российской Федерации продукция средств массовой информации, печатная продукция, аудиовизуальная продукция на любых видах носителей, программы для электронных вычислительных машин (программы для

ЭВМ) и базы данных, а также информация, распространяемая посредством зрелищных мероприятий, посредством информационно-телекоммуникационных сетей, в том числе сети Интернет, и сетей подвижной радиотелефонной связи.

Информация, причиняющая вред здоровью и (или) развитию детей, – информация (в том числе содержащаяся в информационной продукции для детей), распространение которой среди детей запрещено или ограничено в соответствии с настоящим Федеральным законом;

Интернет-травля, или кибертравля (кибербуллинг) – намеренные оскорбления, буллинг, угрозы, диффамации и сообщение другим компрометирующих данных с помощью современных средств коммуникации, как правило, в течение продолжительного периода времени.

Классификация информационной продукции – распределение информационной продукции в зависимости от её тематики, жанра, содержания и художественного оформления по возрастным категориям детей в порядке, установленном Федеральным законом от 29.12.2010 № 436-ФЗ «О защите детей от информации, причиняющей вред их здоровью и развитию».

Медиа (англ. media, от лат. medium 'посредник') – обширное понятие, включающее в себя средства коммуникации, способы передачи информации, а также образовываемую ими среду (медиапространство).

Натуралистические изображение или описание – изображение или описание в любой форме и с использованием любых средств человека, животного, отдельных частей тела человека и (или) животного, действия (бездействия), события, явления, их последствий с фиксированием внимания на деталях, анатомических подробностях и (или) физиологических процессах.

Оборот информационной продукции – предоставление и (или) распространение информационной продукции, включая её продажу (в том числе распространение по подписке), аренду, прокат, раздачу, выдачу из фондов общедоступных библиотек, публичный показ, публичное исполнение (в том числе посредством зрелищных мероприятий), распространение посредством эфирного или кабельного вещания, информационно-телекоммуникационных сетей, в том числе сети Интернет, и сетей подвижной радиотелефонной связи.

Программы-шпионы – это программное обеспечение, устанавливаемое на компьютере для просмотра и записи действий пользователя. Некоторые виды программ-шпионов записывают нажатия клавиш и сведения, вводимые на веб-сайтах или в других программах, а затем используют эти сведения для распространения целевой рекламы или кражи идентификацион-

ных сведений. Эти программы могут быть установлены на компьютере различными способами или быть скрыты внутри таких программ, как бесплатные игры, заставки и наборы подвижных указателей.

СМИ – средства массовой информации.

Спам – это электронный эквивалент бумажной рекламы, которую бросают в ваш почтовый ящик. Спам опасен, особенно если является частью фишинга.

Фишинг (англ. Phishing от fishing «рыбная ловля, выуживание») – вид интернет-мошенничества, целью которого является получение доступа к конфиденциальным данным пользователей –логинам и паролям.

Эксперт – лицо, привлекаемое для проведения экспертизы информационной продукции и дачи экспертного заключения или осуществления классификации информационной продукции и проведения её экспертизы.

Текст цитируется с сайта: https://www.kaspersky.ru

Инструктивно-методическое издание

ОБЕСПЕЧЕНИЕ МЕДИАБЕЗОПАСНОСТИ В ОБРАЗОВАТЕЛЬНОЙ ОРГАНИЗАЦИИ

Методические рекомендации

Редактор Минова Н.М.
Верстка Кузнецова О.В.

Подписано в печать 06.03.2023
Формат 60×84 1/16 Усл. печ. л. 2,8
Тираж 100 экз.

Отпечатано в типографии
Красноярского краевого института повышения квалификации
и профессиональной переподготовки работников образования

660049, Россия,
г. Красноярск, пр. Мира, 76
Красноярский краевой ИПК РО
Тел. 8(391) 206-99-19 (114)