Министерство образования и науки Челябинской области

Государственное бюджетное учреждение
дополнительного профессионального образования
«Челябинский институт переподготовки и повышения квалификации
работников образования»

Организация медиабезопасности в образовательной организации

Методические рекомендации
для руководителей
образовательных организаций

Челябинск
ЧИППКРО
2018

УДК 371:004
ББК 71.063.14+74.244.4
О-64

Рекомендовано к изданию решением ученого совета
ГБУ ДПО ЧИППКРО

Рецензенты:
С. И. Симакова, заведующий кафедрой журналистики и массовых коммуникаций ЧелГУ, кандидат филологических наук, доцент
Е. В. Киприянова, директор МБОУ «Лицей № 11 г. Челябинска», доктор педагогических наук

О-64 **Организация медиабезопасности в образовательной организации** [Электронный ресурс] : методические рекомендации для руководителей образовательных организаций / Т. А. Абрамовских. – Челябинск : ЧИППКРО, 2018. – 56 с.

В предлагаемых материалах даны рекомендации по организации деятельности руководителя образовательной организации по медиабезопасности, показаны направления деятельности по формированию системы медиабезопасности. Отдельно уделено внимание вопросу медиаобразования как необходимого условия организации медиабезопасности. Методические рекомендации предназначены для руководителей образовательных организаций.

Методические рекомендации подготовлены на основе нормативных актов, регламентирующих деятельность организаций по обеспечению безопасности участников образовательных отношений, с использованием накопленного позитивного опыта работы образовательных организаций системы общего образования в аспекте медиабезопасности.

УДК 371:004
ББК 71.063.14+74.244.4

Содержание

Введение

Современное общество характеризуется постоянно растущим объемом информации, передаваемой по каналам масс-медиа, и неизменной востребованностью этой информации. Левада-Центром накоплены данные о том, откуда россияне получают информацию, какие каналы информации и с какой интенсивностью используют. Представим некоторые статистические данные, утверждающие тенденцию роста значимости средств массовой информации в жизни современного человека. Телевидение на сегодняшний день остается главным источником информации для россиян (на начало 2017 года 91% населения отметили, что «хотя бы раз в неделю» или чаще смотрят новости по телевизору). В самой молодой возрастной группе интернет обогнал телевидение как источник информации (более 70% молодых людей предпочитают получать информацию из интернета). Около трети россиян пользуется социальными сетями ежедневно или практически ежедневно. В самой молодой возрастной группе пользуются социальными сетями хотя бы «несколько раз в неделю» 93% респондентов. Каналы видеоблогеров смотрит около четверти молодых россиян. Однако исследования в области теории и практики медиаобразования показывают, что уровень медиаграмотности населения неадекватен современному информационно насыщенному миру. *Почти половина населения (46%) сомневается в своей способности распознать ложь и правду в информационных потоках. Полностью уверены, что могут разобраться в этом лишь 9%. Еще 44% россиян считают, что большинству населения страны не нужна правда, если она не касается их напрямую.* Таким образом, с развитием сети интернет и медиакоммуникационных каналов на первое место выдвигается *вопрос оценки качества информации*, которую получают пользователи – потребители медиа. Не существует универсальных комплексных решений, которые могли бы обеспечить аудиторию только качественным контентом. В данном контексте проблема медиабезопасности населения становится все более актуальной. Предупреждение проблем в области медиабезопасности в образовательных организациях возможно в условиях системной медиаобразовательной деятельности. Как следствие, целесообразно рассматривать *организацию медиабезопасности* в образовательной организации как одну из *ключевых задач медиаобразования*.

Данные методические рекомендации разработаны для руководителей образовательных учреждений, определивших необходимость организации системы медиабезопасности как обязательного компонента медиакомпетентности всех участников образовательных отношений. Как следствие, они будут интересны разным категориям педагогических работников, родителям в связи с возросшей потребностью обеспечения безопасности детей и подростков при обучении и воспитании, организации внеурочной деятельности и свободном использовании современных информационно-коммуникационных технологий (интернет, сотовая (мобильная) связь и СМИ). Материалы рекомендаций носят универсальный характер. Методические рекомендации разработаны с учетом требований действующего законодательства о безопасности детей.

1. Нормативно-правовые основы медиабезопасности в образовательных организациях

В современном обществе медиабезопасность обучающихся обеспечивается комплексом законодательных актов.

На **международном уровне** безопасность в медийном пространстве гарантируется комплексом нормативно-правовых документов:

– Европейская декларация о свободе обмена информацией в интернете 2003 г.; Европейская рамочная конвенция о безопасном использовании мобильных телефонов маленькими детьми и подростками 2007 г.;

– Рекомендации Европейского Парламента и Совета ЕС от 20.12.2006 о защите несовершеннолетних и человеческого достоинства в Интернете; Решение Европейского парламента и Совета ЕС № 276/1999/ о принятии долгосрочного плана действий Сообщества по содействию безопасному использованию Интернета посредством борьбы с незаконным и вредоносным содержимым в рамках глобальных сетей;

– Европейская декларация о свободе обмена информацией в интернете 2003 г.

– Конвенция о правах ребенка (одобрена Генеральной Ассамблеей ООН 20.11.1989) и др.

В Российской Федерации информационная безопасность детей, защита их физического, умственного и нравственного развития также обеспечиваются рядом нормативно-правовых актов.

В соответствии со статьей 14.1 Федерального закона *«Об основных гарантиях прав ребенка в Российской Федерации»* в целях содействия физическому, интеллектуальному, психическому, духовному и нравственному развитию детей и формированию у них навыков здорового образа жизни органы государственной власти Российской Федерации, органы государственной власти субъектов Российской Федерации, органы местного самоуправления в соответствии с их компетенцией создают благоприятные условия для осуществления деятельности организаций, образующих социальную инфраструктуру для детей (включая места для их доступа к сети интернет).

Федеральный закон № 152-ФЗ «О персональных данных» обеспечивает защиту прав и свобод человека и гражданина при обработке

его персональных данных, в том числе защиту прав на неприкосновенность частной жизни, личную и семейную тайну.

В *Федеральном законе № 390-ФЗ «О безопасности»* определены направления деятельности по обеспечению безопасности*:*

1) определение основных направлений государственной политики и стратегическое планирование в области обеспечения безопасности;

2) прогнозирование, выявление, анализ и оценка угроз безопасности;

3) правовое регулирование обеспечения безопасности;

4) разработка и применение комплекса оперативных и долговременных мер по выявлению, предупреждению и устранению угроз безопасности;

5) применение специальных экономических мер в целях обеспечения безопасности;

6) разработка, производство и внедрение современных видов вооружения, военной и специальной техники, а также техники двойного и гражданского назначения в целях обеспечения безопасности;

7) организация научной деятельности в области обеспечения безопасности;

8) координация деятельности федеральных органов государственной власти, органов государственной власти субъектов Российской Федерации, органов местного самоуправления в области обеспечения безопасности;

9) финансирование расходов на обеспечение безопасности, контроль над целевым расходованием выделенных средств;

10) международное сотрудничество в области обеспечения безопасности и др.

Федеральный закон № 436-ФЗ «О защите детей от информации, причиняющей вред их здоровью и развитию» представляет перечень информации, запрещенной для распространения среди детей. К таковой относят информацию:

1) побуждающую детей к совершению действий, представляющих угрозу их жизни и (или) здоровью, в том числе к причинению вреда своему здоровью, самоубийству;

2) способную вызвать у детей желание употребить наркотические средства, психотропные и (или) одурманивающие вещества, табачные изделия, алкогольную и спиртосодержащую продукцию, принять участие в азартных играх, заниматься проституцией, бродяжничеством или попрошайничеством;

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

4) отрицающую семейные ценности, пропагандирующую нетрадиционные сексуальные отношения и формирующую неуважение к родителям и (или) другим членам семьи;

5) оправдывающую противоправное поведение;

6) содержащую нецензурную брань;

7) содержащую 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.

В *Концепции информационной безопасности* детей определены ожидаемые результаты в рамках медиаобразования: к 2020 году будет создана новая медиасреда, соответствующая следующим характеристикам:

«– 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».

Федеральный закон от 27.07.2006 № 149-ФЗ (ред. от 19.07.2018) «Об информации, информационных технологиях и о защите информации» регулирует отношения, возникающие при осуществлении права на работу с информацией, при применении информационных технологий и обеспечении защиты информации.

В статье 8 данного закона определяется право на доступ к информации: граждане и организации вправе осуществлять поиск и получение любой информации в любых формах и из любых источников при условии соблюдения требований, установленных настоящим федеральным законом и другими федеральными законами.

В статье 9 ФЗ-149 разъясняется ограничение доступа к информации. Обязательным является соблюдение конфиденциальности информации, доступ к которой ограничен федеральными законами.

В деятельности по организации медиабезопасности необходимо руководствоваться еще одним нормативным актом: *Правила подключения общеобразовательных учреждений к единой системе контент-фильтрации доступа к сети интернет, реализованной Министерством образования и науки Российской Федерации от 11.05.2011 № АФ-12/07.*

На региональном уровне были созданы письма Министерства образования и науки Челябинской области «Об организации работы по медиабезопасности» (Письмо от 27.12.2012 № 15/10422 , Письмо от 12.03.2013 № 05/1633). Безопасность работы с интернетом обеспечивает приказ Министерства образования и науки Челябинской области от 06.02.2007 № 01-110 «О внедрении контентной фильтрации доступа образовательных учреждений Челябинской области, подключаемых к сети интернет».

На уровне образовательных организаций в соответствии с законом «Об образовании в Российской Федерации» необходимые локальные акты разрабатываются самостоятельно. Они не должны противоречить федеральным и региональным законам в сфере информационной безопасности. Перечень нормативных актов отражает направления и содержание деятельности образовательной организации по реализации медиаобразования и медиабезопасности. В перечень таковых могут войти:

1. Положение об организации медиабезопасности в образовательной организации.

2. Положение об организации системы медиаобразования в образовательной организации.

3. Инструкции (регламенты) по работе педагогов и обучающихся в сети интернет.

4. Инструкция для сотрудников образовательных организаций о порядке действий при осуществлении контроля использования обучающимися сети интернет.

5. Журнал регистрации работы пользователей в сети интернет, который может включать следующие пункты: № п/п, дата и время выхода в сеть, причина выхода, разрешение на выход ответственным за кабинет (журнал расположен рядом с ПК).

6. Правила безопасной работы в сети интернет.

7. Инструкция по организации антивирусной защиты.

8. Требования к сайту образовательного учреждения.

9. Примерный регламент работы сотрудников муниципального общеобразовательного учреждения с электронной почтой.

Дополнения к должностным инструкциям работников МОУ в части формирования медиакомпетентности и реализации системы медиабезопасности в образовательной организации и др.

2. Государственные органы и общественные организации, занимающиеся проблемами защиты детей в киберпространстве

(Рекомендации Европейского Парламента и Совета ЕС от 20.12.2006 о защите несовершеннолетних и человеческого достоинства в интернете)

В соответствии с Рекомендациями Европейского Парламента и Совета ЕС в данной главе определены наиболее авторитетные организации, занимающиеся проблемами защиты детей и взрослых в медиапространстве.

Центр безопасного интернета является членом Международной сети «горячих линий» по борьбе с противоправным контентом. Центр осуществляет реализацию программы «Безопасный интернет». Основные направления деятельности Центра в соответствии с целями программы: создание «горячей линии» в сети интернет для выявления фактов распространения вредной для детей информации; оказание юридической помощи гражданам Российской Федерации по вопросам, связанным с распространением противозаконной или вредной для детей информации в сети интернет или сетях мобильной телефонной связи; проведение мероприятий по указанным проблемам; создание и поддержка информационных сайтов Программы в сети интернет; сотрудничество с международными организациями, которые определяют целями своей деятельности борьбу с противозаконной и вредной для детей информацией в сети интернет и сетях мобильной телефонной связи (http://www.detivrunete.ru/).

Лига безопасного интернета – крупнейшая в России организация, созданная при поддержке Министерства коммуникаций и связи Российской Федерации для борьбы с опасным контентом во всемирной сети путем самоорганизации профессионального сообщества участников интернет-рынка и рядовых пользователей. Лига занимается проблемами безопасности детей в сети (http://www.ligainternet.ru/).

Фонд развития интернет – организация, целями которой являются: поддержка проектов, связанных с развитием сети интернет; содействие развитию глобальных информационных сетей; содействие развитию правового обеспечения в Сети. Фонд развития интернет осу-

ществляет исследования по проблемам использования ИКТ школьниками, их социализацию в развивающемся информационном обществе. *Журнал «Дети в информационном обществе»* – издательский проект, осуществляемый Фондом развития интернет при научной поддержке факультета психологии МГУ имени М. В. Ломоносова и Федерального института развития образования Министерства образования и науки РФ (http://www.fid.su/).

Интерактивная Линия помощи «Дети онлайн» – всероссийский общественный проект, который включает службу телефонного и онлайн консультирования по проблемам безопасного использования сети Интернет и мобильной связи для всех участников образовательных отношений: обучающихся, родителей и работников образовательных учреждений. *Обратившись на Линию, пользователи могут получить квалифицированную помощь специалистов по вопросам безопасного пользования сетью интернет и мобильной связью.* Сайты Линии помощи: www.detionline.com, www.detionline.org.

Управление «К» МВД России – одно из подразделений в составе Бюро специальных технических мероприятий МВД РФ, занимающееся раскрытием преступлений в сфере высоких технологий. Компетенции Управления «К» распространяются на следующие виды преступлений:

– противоправные действия в сфере компьютерной безопасности (мошенничество с платежными системами, неправомерное использование информации, изготовление и распространение вредоносных программ, распространение в интернете порнографии с участием несовершеннолетних);

– преступления в информационно-телекоммуникационных сетях (незаконное использование ресурсов сетей сотовой и проводной связи, интернета, спутникового и кабельного телевидения);

– незаконное использование специальных технических и радиоэлектронных средств;

– нелицензированное программное обеспечение, нарушение авторских прав;

– факты преднамеренного нарушения международного права в сфере информационных технологий (http://www.mvd.ru/).

3. Концептуальные и методологические основы медиаобразования и медиабезопасности

Современные исследователи в сфере медиа оставляют неопределенность в определении понятий «медиабезопасность» и «информационная безопасность»: можно ли считать данные понятия синонимами? Предполагается, что для эффективной работы в этой области стоит придерживаться взглядов, что это несколько разные понятия. Определение *информационной безопасности* в обобщенном варианте можно представить как *безопасность внутри информационных ресурсов, защищенность самой информации*. В трактовке И. А. Фатеевой *«медиабезопасность – это один из видов безопасности современного человека, живущего в атмосфере постоянных природных и техногенных рисков, наряду с экологической, дорожной, противопожарной, химической и другими видами безопасности»*. В данном аспекте медиабезопасность понимается как защищенность интересов членов общества от угроз, которые может таить или уже таит в себе медиапространство. В широком смысле *медиабезопасность* – это деятельность, направленная на защиту интересов гражданского общества от появления и распространения недостоверной информации в сети интернет, способной негативно повлиять на социальные процессы. В узком смысле *медиабезопасность* – это деятельность по обеспечению личной безопасности пользователя в сети интернет, которая позволяет ему не только распознавать недостоверную информацию, но и предотвращать распространение вредоносной информации.

Таким образом, *информационная безопасность – это защищенность информации, медиабезопасность – это защищенность пользователей от недостоверной информации.* «*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 Российской Федерации от 29 декабря 2010 года № 436-ФЗ «О защите детей от информации, причиняющей вред их здоровью и развитию»).

С целью минимизации угроз со стороны медиа в исследованиях ученых определяются пути решения проблемы медиабезопасности. На сегодняшний день определены *две основные теоретические моде-*

ли медиабезопасности: медиаобразование и медиаэкология. Наиболее актуальный путь преодоления рисков медиапотребления – медиаобразование в аспекте педагогического подхода. Российская педагогическая энциклопедия определяет *медиаобразование* как направление в педагогике, выступающее за изучение школьниками закономерностей массовой коммуникации (прессы, телевидения, радио, кино, видео и т. д.). Основные задачи медиаобразования: подготовить новое поколение к безопасной жизни в современных информационных условиях, к критическому восприятию различной информации, научить потребителя понимать цели и намерения авторов любой информации, осознавать последствия ее воздействия на психическое здоровье человека, овладевать способами общения на основе невербальных форм коммуникации. *Позитивным результатом медиаобразования следует считать медиакомпетентность личности* – «совокупность ее мотивов, знаний, умений, способностей, способствующих выбору, использованию, критическому анализу, оценке, созданию и передаче медиатекстов в различных видах, формах и жанрах, анализу сложных процессов функционирования медиа в социуме». Современная информация, передаваемая по каналам масс-медиа, профессионально разрабатывается специалистами в этой области и направлена на манипулирование сознанием потребителя информации с различными целями. Для получения необходимой информации пользователю приходится ее «вытягивать» в большом информационном потоке. Культура осмысленной работы с информацией в интернете может формироваться в период обучения в образовательной организации в системе медиаобразования. Таким образом, *медиаобразование* выполняет важную роль в защите детей от негативного воздействия средств массовой коммуникации, значит, является одним из необходимых условий медиабезопасности. *Медиаграмотность* определяется в международном праве как «грамотное использование детьми и их преподавателями инструментов, обеспечивающих доступ к информации, развитие критического анализа содержания информации и привития коммуникативных навыков, содействие профессиональной подготовке детей и их педагогов в целях позитивного и ответственного использования ими информационных и коммуникационных технологий и услуг» (Рекомендация Комитета министров государствам-членам Совета Европы по расширению возможностей детей в новой информационно-коммуникационной среде от 27.09.2006).

Как следствие, аудитория, находящаяся на более высоком уровне медиаграмотности, обладает более высоким уровнем понимания, управления и оценки медийного мира (Potter, 2001, p. 120).

В связи с необходимостью повышения медиакомпетентности педагогов представляется важным определить основные теоретические подходы, которые нашли наиболее широкое распространение в истории отечественного медиаобразования. Знание теоретических подходов к организации медиаобразования может стать платформой для разработки системы медиабезопасности в образовательной организации. В современной отечественной медиапедагогике выделяется несколько медиаобразовательных подходов: социокультурный, «развития критического мышления», «инъекционный», «удовлетворения потребностей», «практический», идеологический, семиотический, культурологический, эстетический, этический и др. Каждый из подходов может быть реализован в практике медиаобразования.

Например, *«инъекционная»* теория утверждает, что средства массовой информации оказывают на пользователя значительное вредное воздействие. Цель данной теории состоит в смягчении негативного эффекта медиа. Для реализации данной цели аудитории предлагаются конкретные примеры негативного влияния медиа. Основная идея данной теории заключается в том, что аудитория состоит из пассивных потребителей, которые, как правило, не могут понять суть медиатекста. Главная задача состоит в том, чтобы «защищать», «ограждать» их от вредного влияния медиаинформации.

Сторонники *«практической»* теории медиаобразования выдвигают на первый план изучение медиатехники и ее практическое освоение. Однако в аспекте данной теории необходимо обратить внимание на тот факт, что кроме формы (детали, механизмы, техническое устройство и т. д.), медиа имеют содержание, которое необходимо осознать для активного использования. Главная цель медиаобразовательной концепции *«удовлетворения потребностей»* – помощь аудитории в извлечении из медиа максимума полезного в соответствии со своими потребностями, реализация возможности приобрести с помощью медиа необходимые знания, умения, навыки. Однако медиатексты часто несут большую смысловую нагрузку, требующую всестороннего анализа и осознания, что возможно только при условии должной медиакомпетентности. В последние годы значительный интерес появился к *теории «развития критического мышления»*, цель которой – научить

«ориентироваться в информационном потоке», а также предупредить возможность манипуляции сознанием аудитории со стороны медийных источников. Умение критически осмысливать, анализировать медиаинформацию, «грамотно понимать ее, иметь представления о ее механизмах и последствиях ее влияния на зрителей, читателей, слушателей» становится очень важным фактором безопасности в современном информационном мире. *Семиотическая* теория медиаобразования определяет свое главное предназначение в том, чтобы научить аудиторию «прочитывать» медиатекст, представляющий собой многозначный знаковый комплекс. В процессе медиаобразования пользователи СМИ должны научиться расшифровывать (декодировать) различные виды медиаинформации. Сторонники *культурологической теории* утверждают, что ознакомление с ключевыми понятиями, стереотипами, распространяемыми с помощью медиа; работа с медиапроизведениями направлена на выработку оценки и критического, самостоятельного анализа. Основные положения *этической теории* предполагают формирование определенных этических принципов аудитории посредством медиа, приобщение аудитории к определенной этической модели поведения. *Социокультурная теория* представляет собой синтез основных позиций культурологического и социологического теоретических подходов. Данный подход ориентирован на осмысление социальной роли медиа и необходимость обучения медиаязыку широких слоев общества; на профессиональную подготовку и расширение возможностей медиапедагогической деятельности в различных сферах социума.

В практике российского медиаобразования в «чистом виде» теории довольно редко встречаются, как правило, они синтезируются, составляя теоретическую основу определенной концепции медиаобразования, способствуя развитию медиаграмотности аудитории. Эффективность системы безопасности образовательной организации, уровень просвещения педагогов, обучающихся, родителей в области медиабезопасности зависят от созданных в образовательной организации условий и системности мероприятий в рамках основных направлений деятельности по организации медиаобразования.

4. Основные направления деятельности образовательной организации по медиабезопасности

В целях создания организационно-управленческих условий по организации медиабезопасности в образовательной организации рекомендуется определить следующие направления:

1. Нормативно-правовое обеспечение медиабезопасности (подготовка нормативных документов, регламентирующих организацию работы по медиабезопасности в общеобразовательной организации (см. пункт 1 настоящих рекомендаций).

2. Осуществление в образовательных организациях блокирования информационных каналов проникновения в подростковую среду материалов криминальной психологии, культа жестокости и насилия, других антиобщественных и асоциальных тенденций и соответствующей им символики через установление контент-фильтрации. При выборе контент-фильтрации руководителям образовательных организаций необходимо руководствоваться ст. 5 Федерального закона № 436-ФЗ «О защите детей от информации, приносящей вред их здоровью и развитию», где размещен перечень видов информации, причиняющей вред здоровью и (или) развитию детей».

3. Осуществление просветительской и консалтинговой работы с родителями о необходимости контроля за использованием сети интернет и установки контент-фильтров на домашние компьютеры.

5. Внедрение мониторинговых исследований по вопросам обеспечения безопасности образовательной среды при использовании информационно-компьютерных средств в образовательной деятельности.

6. Организация медиаобразования участников образовательных отношений как основного механизма формирования медиакомпетентности, что составляет гарантию безопасности в информационном поле.

6.1. Формирование и развитие компетенций обучающихся в области использования информационно-коммуникационных технологий на уровне общего пользования, включая владение информационно-коммуникационными технологиями, поиском, построением и передачей информации, презентацией выполненных работ, основами информационной безопасности, умением безопасного использования средств информационно-коммуникационных технологий и сети ин-

тернет через внедрение программ обучения детей и подростков *правилам безопасного поведения в интернет-пространстве, профилактике интернет-зависимости.*

6.2. Успешность наших детей, сформированные нравственные принципы, их гражданская позиция во многом будут определяться уровнем медиакомпетенций педагогов, которые в рамках требований профессиональных стандартов становятся обязательным элементом общей профессиональной культуры учителя. Можно выделить основные медиакомпетенции:

1) умение создавать медиатексты, анализировать и интерпретировать их;

2) определение источников медиатекстов, понимание их контекста;

3) интерпретирование нравственных ценностей, распространяемых медиа;

4) умение выбирать соответствующие медиа для создания своих собственных текстов и формирования собственной целевой аудитории;

5) свободное владение средствами масс-медиа с целью их восприятия и использования в своей деятельности.

Обобщенный перечень медиакомпетенций педагога, данный в исследованиях ученых – основателей отечественной школы медиаобразования, нашел свое отражение в требованиях профессиональных стандартов педагогов (см. табл. 2 в приложении).

5. Система деятельности руководителя по реализации медиаобразования в образовательной организации

Медиаобразование выполняет важную функцию защиты от противоправного и манипулятивного воздействия средств массовой коммуникации, а также способствует предупреждению криминальных посягательств на детей с использованием информационно-телекоммуникационных сетей.

Системообразующий образовательный эффект может быть достигнут, если учесть следующие основные направления и ключевые позиции в управленческой деятельности руководителя по введению медиаобразования:

1. Нормативно-правовое обеспечение введения медиаобразования требует от руководителя корректировки действующих или создания новых локальных актов в соответствии с необходимостью актуализации проблемы медиаграмотности и требованиями профессиональных стандартов, в которые включены медиакомпетенции. Предметом нормотворческой деятельности руководителя будут: трудовой договор, должностная инструкция, график работы, различные Положения и инструкции

2. Медиаобразование должно стать одним из важных направлений стратегии развития ОО, должно найти свое отражение в стратегическом и тактическом планировании деятельности ОО – в программе развития, в годовом плане работы образовательной организации, в плане методической работы и т. д.

3. Медиобразование в образовательной организации предполагает формирование медиакомпетентности всех участников образовательных отношений, в т. ч. родителей. Организация работы с родителями в сфере медиаобразования должна быть направлена на освоение семейной медиаграмотности; разработку рекомендаций, которые помогут лучше построить занятия с детьми по развитию медиаграмотности, пониманию медиатекстов и позволят использовать в полной мере развивающий, воспитательный и образовательный потенциал медиакультуры.

4. Руководитель должен определить, как будет развиваться медиаобразование в образовательной организации. Теоретические ис-

следования определяют два направления развития медиаобразования в образовательной организации:

– на базовом уровне – как надпредметная образовательная область, которая представлена в концепции интегрированного образования (интеграция медиаобразования с базовым);

– на уровне дополнительного образования – это школьные кружки, журналистские или анимационные студии, школьное телевидение и др.

В обоих случаях рассматриваются методы работы с текстами масс-медиа и решаются общие проблемы деятельности с медиаинформацией: освоение способов работы с материалами СМИ; создание текстов для газет, журналов, видеофильмов; обучение анализу материалов масс-медиа; критическое и уважительное отношение к альтернативным взглядам. Если позволяют ресурсы, можно эти направления объединить.

5. Реализация выбранных направлений требует выбора технологий и механизмов деятельности в области медиаобразования. В исследованиях А. В. Федорова, И. В. Челышевой мы находим описание существующих в России перспективных и адаптированных к российским условиям медиаобразовательных моделей, которые можно использовать в процессе образования и воспитания. Обозначим некоторые из них.

Медиаобразовательная модель Ю. Н. Усова описана как «система использования средств массовой коммуникации и информации (печати, радио, кино, телевидения, видео, компьютерной техники, фотографии) в развитии индивидуальности школьника». Ю. Н. Усову принадлежит и разработка учебной модели развития виртуального мышления, в основу которой положено единство видеосъемки и восприятия ее результатов.

Медиаобразовательная модель А. В. Шарикова представлена как «обучение теории и практическим умениям для овладения современными средствами массовой коммуникации, рассматриваемыми как часть специфической и автономной области знания в педагогической теории и практике; его следует отличать от использования вспомогательных средств в преподавании других областей знания, таких как, например, математика, физика, география и т. п.».

Медиаобразовательная (аспектная) модель А. В. Спичкина практически совпадает с определением А. В. Шарикова. Концептуальной основой данной модели является теория развития «критического

мышления», семиотическая, культурологическая теории медиаобразования.

Медиаобразовательная модель Л. С. Зазнобиной определяется как подготовка «обучающихся к жизни в информатизированном пространстве путем усиления медиаобразовательной аспектности при изучении различных учебных дисциплин».

Каждая модель, как правило, включает в себя цикл творческих и игровых заданий, которые могут использоваться педагогами как в учебной, так и во внеучебной деятельности. Занятия, предложенные в названных моделях, могут проходить в форме уроков, факультативных занятий, спецкурсов, интегрированных в различные учебные предметы, во внеурочную и кружковую деятельность. Сфера применения современных моделей медиаобразования достаточно широка: школы, вузы, учреждения дополнительного образования и досуговой деятельности.

6. Для реализации медиаобразовательных моделей в образовательной организации руководителю необходимо создать кадровые условия: подготовка учителей-предметников, владеющих медиакомпетенциями; педагогов дополнительного образования, способных разрабатывать и реализовывать медиаобразовательные программы; медиапедагогов. В системе непрерывного профессионального развития разработана подготовка педагогов в трех направлениях.

Первое направление – система внутриорганизационного повышения квалификации педагогов в аспекте медиаобразования, которое станет одним из элементов обновления методической работы в самообучающейся организации. Систему работы по формированию медиакомпетентности можно условно разделить на 2 этапа. Первый этап – пропедевтический, ориентированный на формирование информационной культуры. В данном контексте рассматриваются способы работы с информацией, этические и нравственные проблемы деятельности, вырабатывается ответственность за свою деятельность. Второй этап – медиаобразовательный, включающий учебную деятельность с медиатекстами. Содержание обучения связано с информацией и методами ее познания. Медиатексты как средство информации необходимо рассматривать с точки зрения учителя, который несет новые знания ученикам, и с точки зрения самих учащихся, которые посредством разного вида информации адаптируются к окружающему миру и его познанию. Педагогическая задача – понять значение

информации и определить функциональные педагогические возможности ее как средства обучения. Существует целый ряд обязательных требований к использованию масс-медиа в учебном процессе. Следует обратить внимание, что специфика разных видов информации определяет выбор методических приемов и технологий обучения.

Второе направление – повышение квалификации педагогов вне образовательной организации. Данное направление предполагает обучение по дополнительным профессиональным программам по медиаобразованию, которые реализуются в вузах, институтах повышения квалификации и переподготовки кадров, в методических центрах и т. д.

Третье направление – подготовка студентов в вузах, в т. ч. педагогических. Подготовка медиапедагогов и учителей-предметников, обучающихся по программам, формирующим медиакомпетенции.

Обучение можно осуществлять через формальное, неформальное и информальное образование. Такой подход предполагает многоаспектность форм профессионального развития: реализация стандартных дополнительных профессиональных программ; самообразование; обучение на стажировочных площадках; подготовка в рамках сетевой школы консультантов; участие в профессиональных конкурсах; проведение форумов, мастер-классов, конференций, семинаров; реализация научно-прикладных проектов и т. д. Работу с кадрами руководитель начинает с формирования мотивации педагогов к деятельности в медиаобразовательной среде. Выстраивается целая система социальной мотивации, которая требует много усилий управленческой команды и отдельного описания.

7. Создание репозитория медиаобразовательных технологий. Разработанный комплекс медиаобразовательных приемов, методов и технологий обучения хранится в виде файлов, доступных для дальнейшего распространения по локальной сети образовательной организации. Созданный информационный ресурс должен помочь учащимся осваивать медиаграмотность, а педагогам – решать медиаобразовательные задачи в педагогической практике. Опыт работы в сфере медиаобразования позволит дополнять и расширять созданный репозиторий, содержательными элементами которого могут быть: медиаобразовательная практика, диагностические методики, медиатехнологии, медиаобразование в системе компетентностного подхода, медиаобразование и ИКТ, создание авторских медиасредств, ме-

диаобразование и гуманитарные предметы, медиаобразование и естественно-научные предметы, медиаобразование в дошкольном учреждении и т. д.

8. Решению основных задач медиаобразования позволяет, в первую очередь, развитая материально-техническая база образовательной организации: современные компьютеры, объединенные в локальную сеть и обеспечивающие постоянный выход в интернет; мультимедийные проекторы в комплекте с ноутбуками, которые могут быть использованы для демонстрации медиатекстов в любой аудитории школы; интерактивные доски, помогающие совместить процесс демонстрации и создания медиатекста; наличие видеокамер и фотоаппаратов, позволяющих фиксировать моменты школьной жизни и создавать собственные медиапродукты и др. Профессиональный и ответственный подход к подбору программного обеспечения, сочетание лицензированного и свободно распространяемого обеспечения позволяет создавать медиапродукты высокого уровня.

9. Организация контроля за реализацией цели по введению медиаобразования в деятельность ОО как структурного элемента внутренней системы оценки качества образования (ВСОКО). Определение показателей эффективности процесса внедрения медиаобразования в образовательную деятельность.

10. Прогнозирование результатов. К ожидаемым результатам можно отнести:

– формирование процесса образования и развития личности с помощью и на материале средств массовой коммуникации;

– формирование культуры общения с медиаресурсами;

– формирование творческих, коммуникативных способностей, критического мышления, умений интерпретации, анализа и оценки медиатекста;

– обучение различным формам самовыражения при помощи медиатехнологии и медиатехники;

– создание видеостудии для проведения видео- и телеконференций, создания видеофильмов и видеоуроков и т. д.

11. Описание деятельности руководителя по внедрению медиаобразования в образовательную деятельность ОО в форме программы, проекта, дорожной карты.

6. Технология организации медиабезопасности в образовательной организации

Организация любой деятельности ориентирована на два вопроса: что делать? как это делать? Для ответа на вопрос «как это делать?» нужно знать, в какой форме будет осуществляться деятельность и какие средства, способы и подходы при этом будут использоваться. В условиях системных преобразований наряду с традиционными формами деятельности появились новые подходы к организации образовательных процессов. В аспекте современных нормативных требований наиболее актуально применение технологического подхода, основу которого составляет понятие «технология» (от греч. techne – искусство, мастерство, умение, logos – учение). Технология представляет собой процесс последовательного, пошагового осуществления разработанного на научной основе решения какой-либо производственной или социальной проблемы. Технологический подход способствует более четкому представлению внутренних творческих и организационных процессов подготовки и организации любой деятельности. Применение конкретных технологий позволяет:

– анализировать и систематизировать на научной основе практический опыт и его использование;

– комплексно решать творческие и организационные проблемы;

– прогнозировать результаты деятельности, снижать влияние неблагоприятных обстоятельств;

– выбирать наиболее эффективные и разрабатывать новые технологии;

– оптимально использовать имеющиеся в распоряжении ресурсы.

Каждый руководитель, принимая управленческое решение разного уровня, организует различные виды деятельности. При всем многообразии ситуаций можно определить общий алгоритм действий руководителя, который важно иметь в виду, когда организуется деятельность.

Технология организации деятельности

1. Изучение реального состояния дел.
2. Анализ ситуации, определение проблем и поиск механизмов их преодоления.
3. Целеполагание.
4. Стратегическое и тактическое планирование.
5. Реализация разработанных планов.
6. Анализ и оценка результатов.

Технология осуществления деятельности представляет цикличность ее организации. Деятельность является непрерывной и, завершая определенные действия, подводя итог выполненной работы, управленческая команда осуществляет анализ ситуации, которая сложилась на данный момент, для того чтобы поставить новые цели деятельности с учетом предыдущих результатов. Все элементы организации деятельности тесно взаимосвязаны. Данный процесс может осуществляться на разных уровнях, в разные периоды времени, с участием разных категорий участников образовательных отношений (обучающихся, родителей, педагогов). Безусловно, в каждом случае имеется специфика действий, используются разные технологии организации деятельности в целом и на каждом ее этапе. Знание этих технологий и умение их применять позволяют руководителю и педагогическому коллективу повышать эффективность деятельности, добиваться намеченных целей и результатов. При организации системы медиабезопасности в образовательной организации важно найти рациональную меру соотношения управляющих действий со стороны руководителя, педагогов и самоуправления своей деятельностью со стороны обучающихся и родителей с целью педагогически эффективной организации взаимодействия участников образовательной деятельности в каждой конкретной ситуации.

Организация медиабезопасности в ОО будет иметь положительный образовательный эффект в условиях системности и четкой регламентированности, направленной на результат. В данной ситуации наиболее актуальными формами организации станут: дорожная карта, проект, программа (подпрограмма программы развития).

Итак, при организации медиабезопасности можно использовать метод «дорожной карты». Как определяет М. Джемала, «дорожная карта» – это некий процесс обучения, посредством которого члены какой-либо группы выявляют пробелы или новые возможности в отдельных интересующих их сферах. На основе подхода М. Джемала, дорожная карта образовательной организации по реализации какого-либо приоритетного направления деятельности (в нашем случае – медиаобразование) должна отражать разные аспекты планирования: научное, технологическое, продуктное, долгосрочное планирование, планирование возможностей, планирование интеграции, планирование программ, планирование процессов. Можно констатировать, что дорожная карта образовательной организации по реализации медиабезопасности – это разновидность плана. Создание дорожной карты –

это восходящий процесс, позволяющий различным участникам образовательных отношений и социальных партнеров разделить видение долгосрочного планирования и принять в нем посильное участие. Использование дорожной карты – это своего рода «ответный» деловой процесс, который предоставляет организациям возможность реагирования на меняющиеся условия в реальном времени. Согласно теории М. Джемала дорожная карта образовательной организации по реализации какого-либо проекта (в частности – медиабезопасности) должна отражать многоуровневое видение, которое включает в себя временной уровень («знаю когда»), целевой уровень («знаю зачем»), уровень поставок («знаю что») и уровень ресурсов («знаю как»).

Использование проектной технологии по организации медиабезопасности позволит осуществить ознакомление участников образовательного процесса с основными источниками угроз, законодательной базой обеспечения информационной безопасности и формирование умений организовывать собственную информационную деятельность, планируя ее результаты, обеспечивая свою информационную безопасность в Сети.

Цель проекта: привлечь внимание учащихся, их родителей и педагогов к необходимости обеспечения личной информационной безопасности, а также разработка мер и рекомендаций для повышения уровня знаний в плане безопасного, этичного и ответственного использования интернета. Целевой аудиторией проекта являются участники образовательного процесса: педагоги, учащиеся и их родители.

Ожидаемые результаты относительно педагогов: повышение компетентности в сфере проектирования безопасных информационно-образовательных сред и здоровьесберегающего сопровождения образовательного процесса. Представленный проект позволит педагогам разнообразить формы работы с учащимися и их родителями внутри школы, таким образом, чтобы эта деятельность была для них значима. *Учащиеся научатся*: отличать достоверные сведения от недостоверных, вредную для них информацию от безопасной; избегать навязывания им информации, способной причинить вред их здоровью, нравственному и психическому развитию, чести, достоинству и репутации; применять эффективные меры самозащиты от нежелательных для них информации и контактов в сетях. *Родители получат*: знания о видах информации, способной причинить вред здоровью и развитию детей; навыки профилактики и коррекции зависимого поведения детей, связанного с компьютерными

технологиями и интернетом; информацию о способах осуществления родительского контроля в интернете с помощью различного программного обеспечения (ПО); возможность получить консультацию педагога-психолога, инженера по ИКТ и других специалистов.

Традиционной формой организации медиабезопасности может стать программа. При разработке программы необходимо учесть актуальные нормативные акты, современные тенденции в медиасреде, основные мероприятия по реализации программы (см. табл. 1 в приложении). Предлагаем аналоговую модель замысла программы.

ПРОГРАММА
Организация медиабезопасности в образовательной организации (аналоговая модель замысла программы)

Наименование программы	Организация медиабезопасности в образовательной организации
Нормативно-правовая база программы	Смотрите п. 1 рекомендаций
Сроки реализации	Например, 2018–2021 гг.
Разработчики программы	Фамилия, имя, отчество авторов
Исполнители программы	– заместители директора по УВР и по ВР; – учитель информатики и ИКТ; – учителя-предметники; – классные руководители 1–11 классов; – технические специалисты (системный администратор, лаборант) и др.
Цели программы	Формирование безопасной медиасреды школы, обеспечение информационной безопасности учащихся, использующих интернет в образовании и пропаганда безопасного поведения в Сети всех участников образовательных отношений
Задачи программы	– изучение нормативно-правовых документов по вопросам защиты детей от информации, причиняющей вред их здоровью и развитию; – формирование и расширение медиакомпетенций педагогических работников в области медиабезопасного поведения обучающихся; – организации просветительской работы с родителями и общественностью по медиабезопасности

Библиографический список

Литература:

1. Абрамовских, Т. А. Медиаобразование как условие реализации требований профессиональных стандартов по формированию медиакомпетенций педагогических работников образовательных организаций / Т. А. Абрамовских // Актуальные вопросы теории и практики медиаобразования в педагогической сфере : сборник трудов международного форума «Медиаобразование в педагогической сфере: опыт и новые подходы к управлению». Москва, 16–17 марта 2017 г. / под ред. И. В. Жилавской, И. А. Фатеевой. – М. : МГПУ, 2017. – 464 с.

2. Абрамовских, Т. А. Медиаобразование педагогических работников в аспекте профессиональных стандартов [Электронный ресурс] / Т. А. Абрамовских // Научно-методический электронный журнал «Концепт». – 2017. – Т. 31. – С. 1031–1035. – URL: http://e-koncept.ru/2017/970221.htm (дата обращения: 18.02.2018).

3. Абрамовских, Т. А. Организация деятельности руководителя по введению медиаобразования как направления развития образовательной организации в условиях становления информационного общества / Т. А. Абрамовских // Знак: проблемное поле медиаобразования. – Челябинск, 2018. – № 2 (28). – С. 7–16.

4. Беки, Уорли. Интернет: реальные и мнимые угрозы / Уорли Беки ; пер. с англ. – М. : КУДИЦ-ОБРАЗ, 2004. – 320 с.

5. Волков, Д. Российский медиаландшафт: основные тенденции использования СМИ – 2017 [Электронный ресурс] / Д. Волков, С. Гончаров // Аналитический центр Юрия Левады «Левада-Центр». – URL: http:// www.levada.ru (дата обращения: 18.02.2018).

6. Галатенко, В. А. Основы информационной безопасности : учеб. пособие / В. А. Галатенко. – 4-е изд. – М. : Бином. Лаборатория знаний, Интуит, 2008. – 205 с.

7. Джемала, М. Корпоративная «дорожная карта» – инновационный метод управления знаниями в корпорации / М. Джемала // Российский журнал менеджмента. – 2008. – Том 6. – № 4. – С. 149–168.

8. Дзялошинский, И. М. Экология медиапространства: проблемы безопасности и рационального использования коммуникативных ресурсов / И. М. Дзялошинский // Журналист. Социальные коммуникации. – 2014. – № 3 (15). – С. 5–26.

9. Masterman, L., 1988; по Жилавская, И. В. Медиаобразование молодежной аудитории / И. В. Жилавская. – Томск : ТИИТ, 2009. – С. 73–74.

10. Морозова, А. А. Особенности и перспективы повышения медиаграмотности студентов вузов непрофильных (нежурналистских) факультетов. Инновации в системе высшего образования : материалы IV Всерос. науч.-метод. конф. / НОУ ВПО «Челяб. ин-т экономики и права им. М. В. Ладошина» ; отв. ред. А. В. Федоров ; редкол.: С. Б. Синецкий, Г. И. Ладошина, А. Е. Сомов. – Челябинск, 2013. – С. 34–37.

11. Российская педагогическая энциклопедия: В 2 т. Т. 2. М–Я / ред. В. В. Давыдов. – М. : Большая Российская энциклопедия, 1993–1999 . – С. 555.

12. Симакова, С. И. Формирование медиабезопасной среды – актуальное направление в системе образования // Высшее образование для XXI века : XII Международная научная конференция. Москва, 3–5 декабря 2015 г. : доклады и материалы. Круглый стол «Современные тенденции медиаобразования» / отв. ред. О. Е. Коханая. – М. : Изд-во Моск. гуманит. ун-та, 2015. – С. 98–101.

13. Симакова, С. И. К вопросу формирования медиаграмотности граждан / С. И. Симакова // Актуальные вопросы теории и практики медиаобразования в педагогической сфере : сборник трудов международного форума «Медиаобразование в педагогической сфере: опыт и новые подходы к управлению». Москва 16–17 марта 2017 г. / под ред. И. В. Жилавской, И. А. Фатеевой. – М. : МПГУ, 2017. – С. 422–434.

14. Федоров, А. В. Медиаобразование в современной России: основные модели / А. В. Федоров, И. В. Челышева // Высшее образование в России. – 2004. – № 8. – С. 34–39.

15. Федоров, А. В. Медиаобразование: история и теория / А. В. Федоров. – М. : МОО «Информация для всех», 2015. – 450 с.

16. Федоров, А. В. Развитие медиакомпетентности и критического мышления студентов педагогического вуза / А. В. Федоров. – М. : Изд-во МОО ВПП ЮНЕСКО «Информация для всех», 2007. – 616 с.

17. Челышева, И. В. Медиаобразование для родителей: освоение семейной медиаграмотности / И. В. Челышева // Научно-популярное издание. – Таганрог : Изд-во ТТИ ЮФУ, 2008. – 184 с.

18. Челышева, И. В. Теория и история российского медиаобразования / И. В. Челышева. – Таганрог : Изд-во Кучма, 2006. – 206 с.

Нормативно-правовые документы:

Федеральный уровень

1. Указ Президента Российской федерации от 01.06.2012 № 761 «О национальной стратегии действий в интересах детей на 2012–2017 годы».

2. Федеральный закон «О безопасности» от 28.12.2010 № 390-ФЗ (последняя редакция).

3. Федеральный закон РФ от 29.12.2010 № 436-ФЗ «О защите детей от информации, причиняющей вред их здоровью и развитию».

4. Распоряжение Правительства РФ от 18.10.2007 № 1447-р.

5. Письмо МОиН РФ от 28.09.2011 № АП-1057/07 «О правилах подключения общеобразовательных учреждений к единой системе контент-фильтрации доступа к сети интернет».

6. «Правила подключения общеобразовательных учреждений к единой системе контент-фильтрации доступа к сети интернет, реализованной МОиН РФ» от 11.05.2011 № АФ-12/07 вн.

7. Письмо МОиН РФ от 19.03.2007 № АС-283/03 «О рассылке методических и справочных материалов».

8. Методические и справочные материалы для реализации комплексных мер по внедрению и использованию программно-технических средств, обеспечивающих исключение доступа обучающихся образовательных учреждений к ресурсам сети интернет, содержащим информацию, не совместимую с задачами образования и воспитания.

9. Приказ Министерства труда и социальной защиты РФ от 18 октября 2013 г. № 544н «Об утверждении профессионального стандарта „Педагог (педагогическая деятельность в сфере дошкольного, начального общего, основного общего, среднего общего образования) (воспитатель, учитель)“» [Электронный ресурс]. – Режим доступа: consultant.ru.

10. Приказ Министерства труда и социальной защиты РФ от 10.01.2017 № 10н «Об утверждении профессионального стандарта „Специалист в области воспитания“» (зарегистрирован в Минюсте России 26.01.2017 № 45406) [Электронный ресурс]. – Режим доступа: consultant.ru.

Региональный уровень

1. Приказ МОиН Челябинской области от 06 февраля 2007 г. № 01-110 «О внедрении контентной фильтрации доступа ОУ, подключаемых к сети интернет».

2. Письмо МОиН Челябинской области от 27.12.2012 № 15/10422 «Об организации работы по медиабезопасности».

3. Письмо МОиН Челябинской области от 12.03.2013 № 05/1633 «Об организации работы по медиабезопасности».

Интернет-ресурсы:

1. Бесплатные курсы компьютерной грамотности «Азбука интернета» – www.azbukainterneta.ru.

2. Конкурс школьных интернет-проектов «Классный интернет» – www.safe-internet.ru.

3. Российский конкурс «Позитивный контент» – positivecontent.ru.

4. Проект «Белый интернет» – whiteinternet.info.

5. Кибердружина – www.kiberdruzhina.ru.

6. Горячая линия Роскомнадзора для жалоб на опасный контент – eais.rkn.gov.ru/feedback/.

7. Сайт www.Единыйурок.рф.

8. Безопасность детей в интернете. Nachalka.com 2008 [Электронный ресурс]. – URL: http://www.nachalka.com/bezopasnost.

9. Безопасность дома [Электронный ресурс]. – URL: http://www.microsoft.com/rus/protect/default.mspx.

10. Основы безопасности детей и молодежи в интернете – интерактивный курс по интернет-безопасности. Владельцами авторских прав на сайт являются проект «Финский день информационной безопасности» и WSOYpro [Электронный ресурс]. – URL: http://laste.arvutikaitse.ee/rus/html/copyright.htm.

Приложение

Методические материалы для организации системы медиабезопасности

(из опыта работы образовательных организаций Челябинска и Челябинской области, источник: сеть интернет)

1. Информационная памятка для обучающихся о безопасном поведении и использовании сети интернет

(Министерство образования и науки Российской Федерации, Департамент государственной политики в сфере общего образования, Письмо от 14 мая 2018 г. № 08-1184 «О направлении информации»)

С каждым годом молодежи в интернете становится больше, а школьники – одни из самых активных пользователей Рунета. Между тем, помимо огромного количества возможностей, интернет несет и проблемы. Эта *памятка* должна помочь тебе безопасно находиться в Сети.

Компьютерные вирусы

Компьютерный вирус – это разновидность компьютерных программ, отличительной особенностью которой является способность к размножению. В дополнение к этому, вирусы могут повредить или полностью уничтожить все файлы и данные, подконтрольные пользователю, от имени которого была запущена зараженная программа, а также повредить или даже уничтожить операционную систему со всеми файлами в целом. В большинстве случаев распространяются вирусы через интернет.

Методы защиты от вредоносных программ:

1. Используй современные операционные системы, имеющие серьезный уровень защиты от вредоносных программ.

2. Постоянно устанавливай патчи (цифровые заплатки, которые автоматически устанавливаются с целью доработки программы) и другие обновления своей операционной системы. Скачивай их только с официального сайта разработчика ОС. Если существует режим автоматического обновления, включи его.

3. Работай на своем компьютере под правами пользователя, а не администратора. Это не позволит большинству вредоносных программ инсталлироваться на твоем персональном компьютере.

4. Используй антивирусные программные продукты известных производителей, с автоматическим обновлением баз.

5. Ограничь физический доступ к компьютеру для посторонних лиц.

6. Используй внешние носители информации, такие как флешка, диск или файл из интернета, только из проверенных источников.

7. Не открывай компьютерные файлы, полученные из ненадежных источников. Даже те файлы, которые прислал твой знакомый. Лучше уточни у него, отправлял ли он тебе их.

Сети WI-FI

Wi-Fi – это не вид передачи данных, не технология, а всего лишь бренд, марка. Еще в 1991 году нидерландская компания зарегистрировала бренд WECA, что обозначало словосочетание “Wireless Fidelity”, которое переводится как «беспроводная точность».

До нашего времени дошла другая аббревиатура, которая является такой же технологией. Это аббревиатура Wi-Fi. Такое название было дано с намеком на стандарт высшей звуковой техники Hi-Fi, что в переводе означает «высокая точность».

Да, бесплатный интернет-доступ в кафе, отелях и аэропортах является отличной возможностью выхода в интернет. Но многие эксперты считают, что общедоступные Wi-Fi сети не являются безопасными.

Советы по безопасности работы в общедоступных сетях Wi-fi:

1. Не передавай свою личную информацию через общедоступные Wi-Fi сети. Работая в них, желательно не вводить пароли доступа, логины и какие-то номера.

2. Используй и обновляй антивирусные программы и брандмауер. Тем самым ты обезопасишь себя от закачки вируса на твое устройство.

3. При использовании Wi-Fi отключи функцию «Общий доступ к файлам и принтерам». Данная функция закрыта по умолчанию, однако некоторые пользователи активируют ее для удобства использования в работе или учебе.

4. Не используй публичный WI-FI для передачи личных данных, например для выхода в социальные сети или в электронную почту.

5. Используй только защищенное соединение через HTTPS, а не HTTP, т. е. при наборе веб-адреса вводи именно «https://».

6. В мобильном телефоне отключи функцию «Подключение к Wi-Fi автоматически». Не допускай автоматического подключения устройства к сетям Wi-Fi без твоего согласия.

Социальные сети

Социальные сети активно входят в нашу жизнь, многие люди работают и живут там постоянно, а в Facebook уже зарегистрирован миллиард человек, что является одной седьмой всех жителей планеты. Многие пользователи не понимают, что информация, размещенная ими в социальных сетях, может быть найдена и использована кем угодно, в том числе не обязательно с благими намерениями.

Основные советы по безопасности в социальных сетях:

1. Ограничь список друзей. У тебя в друзьях не должно быть случайных и незнакомых людей.

2. Защищай свою частную жизнь. Не указывай пароли, телефоны, адреса, дату твоего рождения и другую личную информацию. Злоумышленники могут использовать даже информацию о том, как ты и твои родители планируете провести каникулы.

3. Защищай свою репутацию – держи ее в чистоте и задавай себе вопрос: хотел бы ты, чтобы другие пользователи видели, что ты загружаешь? Подумай, прежде чем что-то опубликовать, написать и загрузить.

4. Если ты говоришь с людьми, которых не знаешь, не используй свое реальное имя и другую личную информации: имя, место жительства, место учебы и прочее.

5. Избегай размещения фотографий в интернете, где ты изображен на местности, по которой можно определить твое местоположение.

6. При регистрации в социальной сети необходимо использовать сложные пароли, состоящие из букв и цифр и с количеством знаков не менее 8.

7. Для социальной сети, почты и других сайтов необходимо использовать разные пароли. Тогда если тебя взломают, то злоумышленники получат доступ только к одному месту, а не во все сразу.

Электронные деньги

Электронные деньги – это очень удобный способ платежей, однако существуют мошенники, которые хотят получить эти деньги.

Электронные деньги появились совсем недавно и именно из-за этого во многих государствах до сих пор не прописано про них в законах.

В России же они функционируют и о них уже прописано в законе, где их разделяют на несколько видов – анонимные и не анонимные. Разница в том, что анонимные – это те, в которых разрешается прово-

дить операции без идентификации пользователя, а в неанонимных идентификация пользователя является обязательной.

Также следует различать электронные фиатные деньги (равны государственным валютам) и электронные нефиатные деньги (не равны государственным валютам).

Основные советы по безопасной работе с электронными деньгами:

1. Привяжи к счету мобильный телефон. Это самый удобный и быстрый способ восстановить доступ к счету. Привязанный телефон поможет, если забудешь свой платежный пароль или зайдешь на сайт с незнакомого устройства.

2. Используй одноразовые пароли. После перехода на усиленную авторизацию тебе уже не будет угрожать опасность кражи или перехвата платежного пароля.

3. Выбери сложный пароль. Преступникам будет непросто угадать сложный пароль. Надежные пароли – это пароли, которые содержат не менее 8 знаков и включают в себя строчные и прописные буквы, цифры и несколько символов, такие как знак доллара, фунта, восклицательный знак и т. п. Например, $tR0ng!.

4. Не вводи свои личные данные на сайтах, которым не доверяешь.

Электронная почта

Электронная почта – это технология и предоставляемые ею услуги по пересылке и получению электронных сообщений, которые распределяются в компьютерной сети. Обычно электронный почтовый ящик выглядит следующим образом: имя_пользователя@имя_домена. Также, кроме передачи простого текста, имеется возможность передавать файлы.

Основные советы по безопасной работе с электронной почтой:

1. Надо выбрать правильный почтовый сервис. В интернете есть огромный выбор бесплатных почтовых сервисов, однако лучше доверять тем, кого знаешь и кто первый в рейтинге.

2. Не указывай в личной почте личную информацию. Например, лучше выбрать «музыкальный_фанат@» или «рок2013» вместо «тема13».

3. Используй двухэтапную авторизацию. Это когда помимо пароля нужно вводить код, присылаемый по SMS.

4. Выбери сложный пароль. Для каждого почтового ящика должен быть свой надежный, устойчивый к взлому пароль.

5. Если есть возможность написать самому свой личный вопрос, используй эту возможность.

6. Используй несколько почтовых ящиков. Первый для частной переписки с адресатами, которым ты доверяешь. Это электронный адрес не надо использовать при регистрации на форумах и сайтах.

7. Не открывай файлы и другие вложения в письмах, даже если они пришли от твоих друзей. Лучше уточни у них, отправляли ли они тебе эти файлы.

8. После окончания работы на почтовом сервисе перед закрытием вкладки с сайтом не забудь нажать на «Выйти».

Кибербуллинг или виртуальное издевательство

Кибербуллинг – преследование сообщениями, содержащими оскорбления, агрессию, запугивание; хулиганство; социальное бойкотирование с помощью различных интернет-сервисов.

Основные советы по борьбе с кибербуллингом:

1. Не бросайся в бой. Лучший способ: посоветоваться как себя вести и, если нет того, к кому можно обратиться, то вначале успокоиться. Если ты начнешь отвечать оскорблениями на оскорбления, то только еще больше разожжешь конфликт.

2. Управляй своей киберрепутацией.

3. Анонимность в сети мнимая. Существуют способы выяснить, кто стоит за анонимным аккаунтом.

4. Не стоит вести хулиганский образ виртуальной жизни. Интернет фиксирует все твои действия и сохраняет их. Удалить их будет крайне затруднительно.

5. Соблюдай свою виртуальную честь смолоду.

6. Игнорируй единичный негатив. Одноразовые оскорбительные сообщения лучше игнорировать. Обычно агрессия прекращается на начальной стадии.

7. Бан агрессора. В программах обмена мгновенными сообщениями, в социальных сетях есть возможность блокировки отправки сообщений с определенных адресов.

8. Если ты свидетель кибербуллинга. Твои действия: выступить против преследователя, показать ему, что его действия оцениваются негативно, поддержать жертву, которой нужна психологическая помощь, сообщить взрослым о факте агрессивного поведения в сети.

Мобильный телефон

Современные смартфоны и планшеты содержат в себе вполне взрослый функционал, и теперь они могут конкурировать со стационарными компьютерами. Однако средств защиты для подобных устройств пока

очень мало. Тестирование и поиск уязвимостей в них происходит не так интенсивно, как для ПК, то же самое касается и мобильных приложений.

Современные мобильные браузеры уже практически догнали настольные аналоги, однако расширение функционала влечет за собой большую сложность и меньшую защищенность.

Далеко не все производители выпускают обновления, закрывающие критические уязвимости для своих устройств.

Основные советы для безопасности мобильного телефона:

1. Ничего не является по-настоящему бесплатным. Будь осторожен, ведь когда тебе предлагают бесплатный контент, в нем могут быть скрыты какие-то платные услуги.

2. Думай, прежде чем отправить SMS, фото или видео. Ты точно знаешь, где они будут в конечном итоге?

3. Необходимо обновлять операционную систему твоего смартфона.

4. Используй антивирусные программы для мобильных телефонов.

5. Не загружай приложения от неизвестного источника, ведь они могут содержать вредоносное программное обеспечение.

6. После того как ты выйдешь с сайта, где вводил личную информацию, зайди в настройки браузера и удали cookies.

7. Периодически проверяй, какие платные услуги активированы на твоем номере.

8. Давай свой номер мобильного телефона только людям, которых ты знаешь и кому доверяешь.

9. Bluetooth должен быть выключен, когда ты им не пользуешься. Не забывай иногда проверять это.

Online-игры

Современные онлайн-игры – это красочные, захватывающие развлечения, объединяющие сотни тысяч человек по всему миру. Игроки исследуют данный им мир, общаются друг с другом, выполняют задания, сражаются с монстрами и получают опыт. За удовольствие они платят: покупают диск, оплачивают абонемент или приобретают какие-то опции.

Все эти средства идут на поддержание и развитие игры, а также на саму безопасность: совершенствуются системы авторизации, выпускаются новые патчи (цифровые заплатки для программ), закрываются уязвимости серверов.

В подобных играх стоит опасаться не столько своих соперников, сколько кражи твоего пароля, на котором основана система авторизации большинства игр.

Основные советы по безопасности твоего игрового аккаунта:

1. Если другой игрок ведет себя плохо или создает тебе неприятности, заблокируй его в списке игроков.
2. Пожалуйся администраторам игры на плохое поведение этого игрока, желательно приложить какие-то доказательства в виде скринов.
3. Не указывай личную информацию в профайле игры.
4. Уважай других участников по игре.
5. Не устанавливай неофициальные патчи и моды.
6. Используй сложные и разные пароли.
7. Даже во время игры не стоит отключать антивирус. Пока ты играешь, твой компьютер могут заразить.

Фишинг или кража личных данных

Обычной кражей денег и документов сегодня уже никого не удивишь, но с развитием интернет-технологий злоумышленники переместились в интернет и продолжают заниматься «любимым» делом.

Так появилась новая угроза: интернет-мошенничество или фишинг, главная цель которого состоит в получении конфиденциальных данных пользователей – логинов и паролей. На английском языке phishing читается как фишинг (от fishing – рыбная ловля, password – пароль).

Основные советы по борьбе с фишингом:

1. Следи за своим аккаунтом. Если ты подозреваешь, что твоя анкета была взломана, то необходимо заблокировать ее и сообщить администраторам ресурса об этом как можно скорее.
2. Используй безопасные веб-сайты, в том числе интернет-магазинов и поисковых систем.
3. Используй сложные и разные пароли. Таким образом, если тебя взломают, то злоумышленники получат доступ только к одному твоему профилю в сети, а не ко всем.
4. Если тебя взломали, то необходимо предупредить всех своих знакомых, которые добавлены у тебя в друзьях, о том, что тебя взломали и, возможно, от твоего имени будет рассылаться спам и ссылки на фишинговые сайты.
5. Установи надежный пароль (PI№) на мобильный телефон.
6. Отключи сохранение пароля в браузере.
7. Не открывай файлы и другие вложения в письмах, даже если они пришли от твоих друзей. Лучше уточни у них, отправляли ли они тебе эти файлы.

Цифровая репутация

Цифровая репутация – это негативная или позитивная информация в сети о тебе. Компрометирующая информация, размещенная в интернете, может серьезным образом отразиться на твоей реальной жизни. «Цифровая репутация» – это твой имидж, который формируется из информации о тебе в интернете.

Твое место жительства, учебы, твое финансовое положение, особенности характера и рассказы о близких – все это накапливается в сети. Многие подростки легкомысленно относятся к публикации личной информации в интернете, не понимая возможных последствий. Ты даже не сможешь догадаться о том, что фотография, размещенная 5 лет назад, стала причиной отказа принять тебя на работу. Комментарии, размещение твоих фотографий и другие действия могут не исчезнуть даже после того, как ты их удалишь. Ты не знаешь, кто сохранил эту информацию, попала ли она в поисковые системы и сохранилась ли она, а главное: что подумают о тебе окружающие люди, которые найдут и увидят это. Найти информацию много лет спустя сможет любой – как из добрых побуждений, так и с намерением причинить вред. Это может быть кто угодно.

Основные советы по защите цифровой репутации:

1. Подумай, прежде чем что-то публиковать и передавать у себя в блоге или в социальной сети.

2. В настройках профиля установи ограничения на просмотр твоего профиля и его содержимого, сделай его только «для друзей».

3. Не размещай и не указывай информацию, которая может кого-либо оскорблять или обижать.

Авторское право

Современные школьники – активные пользователи цифрового пространства. Однако далеко не все знают, что пользование многими возможностями цифрового мира требует соблюдения прав на интеллектуальную собственность. Термин «интеллектуальная собственность» относится к различным творениям человеческого ума, начиная с новых изобретений и знаков, обозначающих собственность на продукты и услуги, и заканчивая книгами, фотографиями, кинофильмами и музыкальными произведениями. Авторские права – это права на интеллектуальную собственность на произведения науки, литературы и искусства. Авторские права выступают в качестве гарантии того, что интеллектуальный/творческий труд автора не будет напрасным, даст

ему справедливые возможности заработать на результатах своего труда, получить известность и признание. Никто без разрешения автора не может воспроизводить его произведение, распространять, публично демонстрировать, продавать, импортировать, пускать в прокат, публично исполнять, показывать/исполнять в эфире или размещать в интернете. Использование «пиратского» программного обеспечения может привести к многим рискам: от потери данных к твоим аккаунтам до блокировки твоего устройства, где установлена нелегальная программа. Не стоит также забывать, что существуют легальные и бесплатные программы, которые можно найти в сети.

Десять фактов, которые нужно сообщить детям ради безопасности в интернете

Интернет может быть прекрасным местом как для обучения, так и для отдыха и общения с друзьями. Но, как и весь реальный мир, Сеть тоже может быть опасна. Перед тем как разрешить детям выходить в интернет самостоятельно, следует установить ряд правил, с которыми должен согласиться и ваш ребенок.

Если вы не уверены, с чего начать, вот несколько рекомендаций, как сделать посещение интернета для детей полностью безопасным.

1. Поощряйте детей делиться с вами их опытом в интернете. Посещайте Сеть вместе с детьми.

2. Научите детей доверять интуиции. Если их в интернете что-либо беспокоит, им следует сообщить об этом вам.

3. Если дети общаются в чатах, используют программы мгновенного обмена сообщениями, играют или занимаются чем-то иным, требующим регистрационного имени, помогите ребенку его выбрать и убедитесь, что оно не содержит никакой личной информации.

4. Настаивайте на том, чтобы дети никогда не выдавали своего адреса, номера телефона или другой личной информации, например места учебы или любимого места для прогулки.

5. Объясните детям, что разница между правильным и неправильным одинакова: как в и интернете, так и в реальной жизни.

6. Научите детей уважать других в интернете. Убедитесь, что они знают о том, что правила хорошего поведения действуют везде – даже в виртуальном мире.

7. Настаивайте, чтобы дети уважали собственность других в интернете. Объясните, что незаконное копирование чужой работы – музыки, компьютерных игр и других программ – является кражей.

8. Скажите детям, что им никогда не следует встречаться с друзьями из интернета. Объясните, что эти люди могут оказаться совсем не теми, за кого себя выдают.

9. Скажите детям, что не все, что они читают или видят в интернете, – правда. Приучите их спрашивать вас, если они не уверены.

10. Контролируйте деятельность детей в интернете с помощью современных программ. Они помогут отфильтровать вредное содержимое, выяснить, какие сайты посещает ребенок и что он делает на них.

2. Практические рекомендации по организации образовательного пространства для учащихся, использующих ИКТ технологии в обучении

Технологии обучения детей и подростков, использующих ИКТ технологии в обучении, обладают определенной спецификой. Развитие у таких учащихся познавательных способностей, расширение сферы их учебных интересов с использованием информационных компьютерных ресурсов требует «продвинутых» педагогических технологий:

– специального учебно-методического и дидактического обеспечения;

– создания соответствующих организационных условий;

– подготовки кадров, которые смогут помочь учащимся в обучении;

– подготовки технических возможностей учебного учреждения.

Организационно-методическая работа должна осуществляться не только в учебной, но и во внеучебной деятельности учащихся.

Технологический алгоритм работы с детьми и подростками, готовыми применять в познавательных целях новые информационные технологии, может состоять в следующем:

1) в составлении каталогов интересующих информационных ресурсов;

2) разработке печатных и электронных рекомендаций о способах формулирования запросов и поиска информации;

3) подготовке наборов «развивающих» информационных блоков для учащихся разного возраста.

В связи с задачами обучения увлеченность информационными технологиями граничит с понятием «компьютерной зависимости», поэтому вполне логичен вопрос: в какой момент такая увлеченность

начинает становиться чрезмерной? На данном временно́м этапе феномен компьютерной зависимости нуждается в широком научном исследовании, в условиях экспериментальных лабораторий и во взаимодействии педагогов с психологами и медиками. Актуальным становится создание психодиагностической базы, которая должна строиться с учетом поведенческих, эмоциональных и личностных особенностей учащихся. В критерии диагностики могут входить следующие параметры:

– способность к самоконтролю и саморегулированию;

– развитие рефлексии своей деятельности;

– способность к антиципации: умению предвидеть последствия своих поступков;

– используемые психологические защиты (уход от проблем, перенос вины на других, оправдание, ответная агрессия и т. д.);

– развитость коммуникативных качеств и копинг-поведения.

Организация работы с учащимися предполагает проведение профилактической работы в целях предупреждения появления компьютерной зависимости. Данная профилактическая работа может носить как локальный характер, обеспечивающий предупреждение возможных неблагоприятных последствий, так и индивидуальный характер, направленный на предупреждение возможных неблагополучий индивидуального развития конкретного учащегося через систему психологической службы школы.

3. Памятка по медиабезопасности несовершеннолетних (для родителей)

Интернет – прекрасное место для общения, обучения и отдыха. Но стоит понимать, что, как и наш реальный мир, всемирная паутина так же может быть весьма и весьма опасна.

Приведем несколько рекомендаций, с помощью которых посещение интернета может стать менее опасным для ваших детей:

1. Посещайте интернет вместе с детьми. Поощряйте ваших детей делиться с вами их успехами и неудачами в деле освоения интернета.

2. Объясните детям, что если в интернете что-либо беспокоит их, то им следует не скрывать этого, а поделиться с вами своим беспокойством.

3. Объясните ребенку, что при общении в чатах, использовании программ мгновенного обмена сообщениями (типа ICQ, Microsoft Messenger и т. д.), использовании онлайн-игр и других ситуациях,

требующих регистрации, нельзя использовать реальное имя, помогите вашему ребенку выбрать регистрационное имя, не содержащее никакой личной информации.

4. Объясните ребенку, что нельзя выдавать свои личные данные, такие как домашний адрес, номер телефона и любую другую личную информацию, например, номер школы, класс, любимое место прогулки, время возвращения домой, место работы отца или матери и т. д.

5. Объясните своему ребенку, что в реальной жизни и в интернете нет разницы между неправильными и правильными поступками.

6. Научите ваших детей уважать собеседников в интернете. Убедитесь, что они понимают, что правила хорошего тона действуют одинаково в интернете и в реальной жизни.

7. Скажите им, что никогда не стоит встречаться с друзьями из интернета. Ведь люди могут оказаться совсем не теми, за кого себя выдают.

8. Объясните детям, что далеко не всё, что они могут прочесть или увидеть в интернете, – правда. Приучите их спрашивать о том, в чем они не уверены.

9. Не забывайте контролировать детей в интернете с помощью специального программного обеспечения. Это поможет вам отфильтровывать вредоносное содержание, выяснить, какие сайты на самом деле посещает ваш ребенок и что он там делает.

Советы родителям

Шаг 1: выбирайте сайты, которые можно посещать вашему ребенку, а какие нельзя (блокируйте доступ к неподходящим сайтам).

Шаг 2: увеличьте уровень защиты и конфиденциальности (создайте отдельные учетные записи для разных пользователей).

Шаг 3: следите за тем, какие сайты посещают ваши дети.

Шаг 4: напоминайте детям, чтобы они не общались в интернете с незнакомцами.

Пусть интернет будет вам и вашим детям только в радость!

«Постарайтесь шагать рядом с ребенком по дороге жизни – и ему не нужно будет удирать в виртуальный мир».

4. Как научить детей отличать правду от лжи в интернете? (информация для родителей)

Следует объяснить детям, что нужно критически относиться к полученным из сети интернет материалам, ведь опубликовать информацию в интернете может абсолютно любой человек. Объясните ребен-

ку, что сегодня практически каждый человек может создать свой сайт и при этом никто не будет контролировать, насколько правдива размещенная там информация. Научите ребенка проверять все то, что он видит в сети интернет. Как это объяснить ребенку?

– Начните, когда ваш ребенок еще достаточно мал. Ведь сегодня даже дошкольники уже успешно используют сеть интернет, а значит нужно как можно раньше научить их отделять правду от лжи;

– Не забывайте спрашивать ребенка об увиденном в сети интернет. Например, начните с расспросов, для чего служит тот или иной сайт.

– Убедитесь, что ваш ребенок может самостоятельно проверить прочитанную в сети интернет информацию по другим источникам (по другим сайтам, газетам или журналам). Приучите вашего ребенка советоваться с вами. Не отмахивайтесь от их детских проблем.

– Поощряйте ваших детей использовать различные источники, такие как библиотеки, или подарите им энциклопедию на диске, например «Энциклопедию Кирилла и Мефодия» или Microsoft Encarta. Это поможет научить вашего ребенка использовать сторонние источники информации.

– Научите ребенка пользоваться поиском в сети интернет. Покажите, как использовать различные поисковые машины для осуществления поиска.

Таблица 1

5. Примерный план по реализации программы по медиабезопасности

№ п/п	Мероприятие	Классы	Срок	Ответственные
Работа с обучающимися				
1.	Проведение тематических линеек по медиабезопасности	1–11	Один раз в полугодие	Преподаватель ОБЖ
2.	Разработка памяток для родителей и обучающихся школы «Опасности интернета»	Актив самоуправления	Один раз в четверть	Педагог-организатор
3.	Проведение классных часов по медиабезопасности	1–11	Один раз в четверть	Классные руководители

№ п/п	Мероприятие	Классы	Срок	Ответственные
4.	Проведение тематических минуток на уроках информатики и ОБЖ	8–10	Постоянно	Учителя информатики и ОБЖ
5.	Конкурс презентаций «Безопасный интернет – детям!»	7–10	В соответствии с годовым планом	Педагог-организатор
6.	Ведение информационной странички школьного сайта «Медиабезопасность»	1–11	Постоянно	Тьютор школы
7.	Выпуск тематической газеты по медиабезопасности	1–11	Один раз в год	Педагог-организатор
8.	Анкетирование обучающихся «Безопасность компьютера и мобильного телефона»	1–10	Один раз в год	Педагог-организатор
Работа с родителями				
1.	Проведение тематических общешкольных собраний по медиабезопасности подростков и детей	1–11	В соответствии с годовым планом	Зам. директора по ВР
2.	Анкетирование родителей «Безопасный интернет для ваших детей»	1–10	Один раз в год согласно срокам годового плана	Педагог-организатор
Работа с педагогическим коллективом				
1.	Разработка плана работы по медиабезопасности на учебный год		Август	Зам. директора по ВР
2.	Совещания при директоре по вопросу медиабезопасности		В соответствии с годовым планом	Директор
3.	Педагогический совет по вопросам медиабезопасности		В соответствии с годовым планом	Директор

6. Уроки медиабезопасности

Уроки медиабезопасности планируются в образовательных учреждениях на постоянной основе, начиная с первого класса, в рамках школьной программы (в том числе уроков ОБЖ).

Цель проведения уроков медиабезопасности: обеспечение информационной безопасности несовершеннолетних обучающихся и воспитанников путем привития им навыков ответственного и безопасного поведения в современной информационно-телекоммуникационной среде.

Задачи уроков медиабезопасности:

1) информирование учащихся о видах информации, способной причинить вред здоровью и развитию несовершеннолетних, запрещенной или ограниченной для распространения на территории Российской Федерации, а также о негативных последствиях распространения такой информации;

2) информирование учащихся о способах незаконного распространения такой информации в информационно-телекоммуникационных сетях, в частности, в сети интернет и мобильной (сотовой) связи (в том числе путем рассылки SMS-сообщений незаконного содержания);

3) ознакомление учащихся с международными принципами и нормами, с нормативными правовыми актами Российской Федерации, регулирующими вопросы информационной безопасности несовершеннолетних;

4) обучение детей и подростков правилам ответственного и безопасного пользования услугами интернета и мобильной (сотовой) связи, другими электронными средствами связи и коммуникации, в том числе способам защиты от противоправных и иных общественно опасных посягательств в информационно-телекоммуникационных сетях, в частности, от таких способов разрушительного воздействия на психику детей, как кибербуллинг (жестокое обращение с детьми в виртуальной среде) и буллицид (доведение до самоубийства путем психологического насилия);

5) профилактика формирования у учащихся интернет-зависимости и игровой зависимости (игромании, гэмблинга);

6) предупреждение совершения учащимися правонарушений с использованием информационно-телекоммуникационных технологий.

Ожидаемые результаты

В ходе уроков медиабезопасности дети должны научиться сделать более безопасным и полезным свое общение в интернете и иных информационно-телекоммуникационных сетях, а именно:

– критически относиться к сообщениям и иной информации, распространяемой в сети интернет, мобильной (сотовой) связи, посредством иных электронных средств массовой коммуникации;

– отличать достоверные сведения от недостоверных, вредную для них информацию от безопасной;

– избегать навязывания им информации, способной причинить вред их здоровью, нравственному и психическому развитию, чести, достоинству и репутации;

– распознавать признаки злоупотребления их неопытностью и доверчивостью, попытки вовлечения их в противоправную и иную антиобщественную деятельность;

– распознавать манипулятивные техники, используемые при подаче рекламной и иной информации;

– критически относиться к информационной продукции, распространяемой в информационно-телекоммуникационных сетях;

– анализировать степень достоверности информации и подлинность ее источников;

– применять эффективные меры самозащиты от нежелательных для них информации и контактов в сетях.

Приложение к классному часу по медиабезопасности

– Игра «Ситуация» (по группам).

Ситуации:

6.1. Вы всегда мечтали иметь программу «Фотошоп». Наконец-то вы нашли ее в интернете и скачали. Активируя программу в компьютере, уже перед завершением процесса, вы прочитали следующее сообщение: «Для получения бесплатного сообщения с кодом введите номер вашего мобильного телефона». Как вы поступите?

6.2. Находясь в интернете, вы открыли очень важную для вас страничку. Но компьютер тут же отреагировал: «Этот файл угрожает безопасности вашего компьютера, содержит троянскую программу». Каковы ваши дальнейшие действия?

6.3. На сайте «Одноклассники» вы познакомились с классным парнем (или классной девчонкой). Через некоторое время «новый друг» просит встречи с вами на «нейтральной территории». Опишите ваши действия.

6.4. Для скачивания файла в интернете потребовали введения ваших личных данных. Как вы поступите? (Источник: https://infourok.ru/klassniy-chas-s-prezentaciey-mediabezopasnost-682321.html).

7. «Интернет-зависимости» и их опасность для пользователей сети

Психологами отмечается распространенность в среде пользователей, в том числе несовершеннолетних, случаев болезненного пристрастия к участию в сетевых процессах, так называемой «интернет-зависимости», проявляющегося в навязчивом желании неограниченно долго продолжать сетевое общение. По данным различных исследований, интернет-зависимыми сегодня являются около 10% пользователей во всем мире. Нередко несовершеннолетние настолько привязываются к виртуальному миру и своему вымышленному персонажу, что забывают обо всем остальном. Для подростков интернет как виртуальная среда иногда кажется даже более адекватной, чем реальный мир. Возможность перевоплотиться в некую бестелесную «идеальную личность» открывает для них новые ощущения, которые им хочется испытывать постоянно или все более часто. Зависимость (аддикция) в психологии определяется как навязчивая потребность, ощущаемая человеком, подвигающая к определенной деятельности. Этот термин употребляется не только для определения наркомании, но и применяется к другим областям, типа проблемы азартных игр и интернет-зависимости. Специалисты отмечают, что в некоторой степени указанная зависимость близка к патологической увлеченности азартными играми, а ее деструктивные эффекты схожи с возникающими при алкоголизме и наркомании, однако, в отличие от последних, имеют нехимическое происхождение. Высказывается мнение, что в подавляющем большинстве случаев такая зависимость – не самостоятельное состояние, а синдром в рамках другого психического расстройства. Таким образом, интернет-зависимость (как вид нехимической зависимости) – это навязчивая потребность в использовании интернета, сопровождающаяся социальной дезадаптацией и выраженными психологическими симптомами. Патология проявляется в разрушении обычного образа жизни, смене жизненных ориентиров, появлении депрессии, нарастании социальной изоляции. Происходит социальная дезадаптация, нарушаются значимые общественные связи.

Выделяется 5 основных типов интернет-зависимости с учетом того, к чему сформировалось пристрастие у конкретной личности: «киберсексу», виртуальным знакомствам, сетевым азартным играм, компьютерным играм или навязчивому перемещению по Web-узлам:

1. Навязчивый веб-серфинг – бесконечные путешествия по Всемирной паутине, поиск информации.

2. Пристрастие к виртуальному общению и виртуальным знакомствам – большие объемы переписки, постоянное участие в чатах, веб-форумах, избыточность знакомых и друзей в Сети.

3. Игровая зависимость – навязчивое увлечение компьютерными играми по сети.

4. Навязчивая финансовая потребность – игра по сети в азартные игры, ненужные покупки в интернет-магазинах или постоянные участия в интернет-аукционах.

5. Пристрастие к просмотру фильмов через интернет, когда больной может провести перед экраном весь день, не отрываясь из-за того, что в сети можно посмотреть практически любой фильм или передачу.

Основные признаки интернет-зависимости: 1) чрезмерное, немотивированное злоупотребление длительностью работы в сети, не обусловленное профессиональной, учебной или иной созидательной деятельностью; 2) использование интернета как преобладающего средства коммуникации; 3) создание и эксплуатация виртуальных образов, крайне далеких от реальных; 4) влечение к интернет-играм и (или) созданию вредоносных программ (без какой-либо цели); 5) субъективно воспринимаемая невозможность обходиться без работы в сети.

При появлении указанных выше признаков следует обратиться за медицинской (психологической и (или) психиатрической) помощью, так в запущенном состоянии интернет-зависимость и игромания значительно хуже поддаются коррекции.

Таблица 2

8. Характеристика профессиональной медиакомпетентности педагогических работников, регламентированная профессиональными стандартами (извлечение)

№ п/п	Профессиональный стандарт	ОТФ, ТФ	Компетенции в рамках ТФ
1.	Профессиональный стандарт «Педагог (воспитатель, учитель)»	Педагогическая деятельность по проектированию и реализации образовательно-	*Необходимые умения* Владеть ИКТ-компетентностями: – общепользовательская ИКТ-компетентность;

№ п/п	Профессиональный стандарт	ОТФ, ТФ	Компетенции в рамках ТФ
		го процесса в образовательных организациях дошкольного, начального общего, основного общего, среднего общего образования. Общепедагогическая функция. Обучение. Воспитательная деятельность	– общепедагогическая ИКТ-компетентность; – предметно-педагогическая ИКТ-компетентность (отражающая профессиональную ИКТ-компетентность соответствующей области человеческой деятельности) (например: оценивание качества цифровых образовательных ресурсов (источников, инструментов) по отношению к заданным образовательным задачам их использования; аудио-, видеотекстовая коммуникация (двусторонняя связь, конференция, мгновенные и отложенные сообщения, автоматизированные коррекция текста и перевод между языками). *Необходимые умения* Находить ценностный аспект учебного знания и информации обеспечивать его понимание и переживание обучающимися
		Педагогическая деятельность по проектированию и реализации основных образовательных программ. Модуль «Предметное обучение. Русский язык»	*Трудовые действия* 1. Использование совместно с обучающимися источников языковой информации для решения практических или познавательных задач, в частности, этимологической информации, подчеркивая отличия научного метода изучения языка от так называемого «бытового» подхода («народной лингвистики»).

№ п/п	Профессиональный стандарт	ОТФ, ТФ	Компетенции в рамках ТФ
			2. Моделирование видов профессиональной деятельности, где коммуникативная компетентность является основным качеством работника, включая в нее заинтересованных обучающихся (издание школьной газеты, художественного или научного альманаха, организация школьного радио и телевидения, разработка сценария театральной постановки или видеофильма и т. д.)
2.	Профессиональный стандарт «Специалист в области воспитания» (социальный педагог, ст. вожатый, педагог-организатор, воспитатель, педагог-библиотекарь, тьютор	Организационно-педагогическое обеспечение воспитательного процесса	*Необходимые умения* Проводить мероприятия по развитию информационной культуры обучающихся, организовывать их информационную деятельность. *Необходимые знания* Формы и методы воспитания у детей информационной культуры, организации их информационной деятельности
		Организационно-методическое обеспечение воспитательной деятельности	*Необходимые умения* Осуществлять поиск и отбор актуальных информационных источников с целью методической поддержки воспитательной деятельности
		Библиотечно-педагогическая деятельность в образовательной организации общего образования	*Трудовые действия* Проведение занятий по формированию сознательного и ответственного информационного поведения обучающихся. Реализация мероприятий по обеспечению информацион-

№ п/п	Профессиональный стандарт	ОТФ, ТФ	Компетенции в рамках ТФ
			ной безопасности обучающихся в образовательной организации
		Проведение мероприятий по воспитанию у обучающихся информационной культуры	*Необходимые умения* Проводить занятия, направленные на освоение обучающимися методов поиска и критического анализа информации. *Необходимые знания* Механизмы поиска информации в традиционной библиотечной и электронной среде. Примерное содержание деятельности детских пресс- или медиацентров

9. Тест для выявления степени медиакомпетентности аудитории (Поттер Джеймс)

Поттер Джеймс выделил следующие уровни развития аудитории по отношению к медиа и предложил следующие вопросы к ним.

Познавательный уровень

1. Вспомните ваш любимый телесериал, затем выполните следующие две задачи:

a) составьте список всех важных персонажей и опишите каждого подробно;

b) опишите события, которые, по-вашему, случатся в следующих сериях.

Эмоциональный уровень

2. Все эмоции имеют диапазон подэмоций, или подтипов. Например, эмоция опасения имеет подтипы ужаса, паники, борьбы, страха, испуга, предчувствия, беспокойства, нервозности, осторожности, приступа растерянности, волнения и т. д. Любой из них – тип опасения, но каждый указывает на различный оттенок этого чувства. А сколько подтипов вы можете перечислить для чувства любви? Сколько – для печали?

3. Посмотрите телевизионную передачу и подсчитайте, сколько раз вы видите выражения чувств опасения, любви и печали?

a) когда вы видите выражение одного из этих чувств, способны ли вы классифицировать их подтип?

b) посмотрите несколько различных видов телевизионных программ и отметьте, какие эмоции изображаются там наиболее часто/редко.

Моральный уровень

4. Посмотрите несколько экранных медиатекстов приключенческого жанра, где отчетливо показано антиобщественное поведение (преступление, насилие, ложь). Заметьте, как персонажи совершают эти действия. Пробуйте классифицировать этих персонажей по уровням морального развития:

a) поразмышляйте о медиатексте в целом и попытайтесь выявить намерения авторов и продюсеров; к которому моральному уровню аудитории они обращаются?

b) если бы вы создавали этот медиатекст и хотели ориентироваться на публику с более высоким уровнем медиавосприятия, что вы изменили бы в сценарии? [Potter, 2001, p. 34].

Ключ к оценке результатов тестирования, имея в виду те же уровни развития аудитории в области медиа.

Познавательный уровень

1. Ответы на часть (a) первого вопроса отражают вашу степень прозрачности интеллекта. Посмотрите, сколько персонажей вы перечислили? Сколько прилагательных или описательных фраз вы перечисляли для каждого персонажа? Заметьте разнообразие в описаниях: были ли они целиком основаны на физиологических данных? Или также перечислялись другие признаки типа индивидуальности (одежда, карьера, любимые жесты/особенности и т. д.)? Чем больше вы вспомнили подробностей, тем большее количество информации вы способны воспринимать/анализировать).

Ответы на часть (b) первого вопроса отражают степень флюидности вашего интеллекта. Если вам было трудно размышлять о любых событиях медиатекста, у вас низка флюидность. Если вы показали немалые возможности воображения и творческого потенциала, у вас высокий уровень флюидности интеллекта.

Сравните ваше выполнение задач (a) и (b). Если вы выполнили (a) намного лучше, то у вас развитые способности собрать факты. Если

вы делали намного лучше задание (b), то ваш интеллект флюиден, у вас развитое воображения и поиск новых перспектив. Развитие высокого уровня медиаграмотности требует, чтобы вы увеличили оба из этих типов интеллекта.

Эмоциональный уровень

2. Чем большее количество подэмоций перечислено вами, тем лучше вы настроены к пониманию тонкого изменения чувств, и тем более вы эмоционально грамотны.

3. Чтобы быть способным определить эмоции в других, нужна способность к сочувствию, к ощущению различий среди подэмоций. Теле/кинотексты насыщены эмоциями. Многие из них очень просто определить, но иные подэмоции ощутить труднее. Действительно ли вы были способны ощутить и понять более сложные эмоции? Способны ли вы были увидеть типы эмоций, которые отличают комедии от приключенческих произведений?

Моральный уровень

4. Способны ли вы делать некоторые обобщения о том, на каком уровне развития находится тот или иной медийный персонаж? Если да, то вы можете ясно видеть конкретные примеры и обсуждать ваши выводы, опираясь на них. Тогда вы обладаете моральной грамотностью. Ваша моральная грамотность высока, если вы можете понимать, как можно изменить сюжеты медиатекстов, чтобы заинтересовать аудиторию различных типов медиавосприятия.

10. Возможные опасности, с которыми сопряжен доступ детей к сети интернет (информация для педагогов):

– Неприемлемые материалы. В интернете ребенок может столкнуться с материалами, связанными с сексом, провоцирующими возникновение ненависти к кому-либо или побуждающими к совершению опасных либо незаконных действий.

– Неприятности, связанные с нарушением законов или финансовыми потерями. У ребенка могут обманным путем узнать номер вашей кредитной карточки, и это вызовет финансовые потери. Ребенка также могут склонить к совершению поступков, нарушающих права других людей, что, в конечном счете, приведет к возникновению у вашей семьи проблем, связанных с нарушением законов.

– Разглашение конфиденциальной информации. Детей и даже подростков могут уговорить сообщить конфиденциальную информацию.

Сведения личного характера, такие как имя и фамилия ребенка, его адрес, возраст, пол и информация о семье, могут легко стать известными злоумышленнику. Даже если сведения о вашем ребенке запрашивает заслуживающая доверия организация, вы все равно должны заботиться об обеспечении конфиденциальности этой информации.

– Проблемы технологического характера. По недосмотру ребенка, открывшего непонятное вложение электронной почты или загрузившего с веб-узла небезопасный код, в компьютер может попасть вирус, «червь», «троянский конь», «зомби» или другой код, разработанный со злым умыслом.

Вывод: не спешите доверять любым предложениям в Сети.

Использовать один простой пароль для электронной почты, ICQ или своих аккаунтов в социальных сетях – то же, что ключом от почтового ящика закрывать входную дверь. Оставляя много личной информации в сети, вы рискуете сделать свои персональные данные доступными мошенникам, которые с их помощью могут от вашего имени рассылать электронные письма, вести ICQ-общение, совершать телефонные звонки или, проникнув в ваш компьютер, уничтожить ценные данные.

Выводы:

– Ограничьте объем информации о себе, находящейся в публичном доступе.

– Используйте только сложные пароли.

– Для разных учетных записей и сервисов используйте разные пароли.

– Не передавайте свои логин и пароль третьим лицам.

Учебное издание

Организация медиабезопасности в образовательной организации

Методические рекомендации
для руководителей
образовательных организаций

Ответственный за выпуск А. В. Коптелов
Технический редактор Н. А. Лазариди

ГБУ ДПО «Челябинский институт
переподготовки и повышения квалификации
работников образования»
454091, г. Челябинск, ул. Красноармейская, 88