Федеральное государственное автономное образовательное учреждение дополнительного профессионального образования «Центр реализации государственной образовательной политики и информационных технологий»

МЕТОДИЧЕСКИЕ РЕКОМЕНДАЦИИ

по формированию у обучающихся навыков безопасного поведения в сети «Интернет»

Москва, 2018

СОДЕРЖАНИЕ

СВЕДЕНИЯ ОБ АВТОРАХ

Валюженич Марина Владимировна, старший методист управления реализации государственного задания федерального государственного автономного образовательного учреждения дополнительного профессионального образования «Центр реализации государственной образовательной политики и информационных технологий»; anosova@apkpro.ru

Гиренко Александр Федорович, начальник отдела информационного сопровождения федерального государственного автономного образовательного учреждения дополнительного профессионального образования «Центр реализации государственной образовательной политики и информационных технологий»; girenko@apkpro.ru

Симонов Александр Васильевич, к.г.н., начальник отдела информатизации прикладных научных исследований федерального государственного автономного образовательного учреждения дополнительного профессионального образования «Центр реализации государственной образовательной политики и информационных технологий»

ТЕОРЕТИЧЕСКИЕ АСПЕКТЫ ФОРМИРОВАНИЯ У ОБУЧАЮЩИХСЯ НАВЫКОВ БЕЗОПАСНОГО ПОВЕДЕНИЯ В СЕТИ ИНТЕРНЕТ

Система образования – курс на цифровизацию.

Современный мир подвержен глобальным изменениям, оказывающим вливание на все социальные процессы. Одна из важных мировых тенденций – цифровизация всех сфер экономики.

На сегодняшний день странами-лидерами по развитию цифровой экономики являются Норвегия, Швеция и Швейцария, также значительные успехи демонстрируют США, Великобритания, Дания, Финляндия, Сингапур, Южная Корея и Гонконг. Россия в рейтинге цифровых экономик мира занимает 39-е место, соседствуя с Китаем, Индией, Малайзией. Однако, согласно данным исследования Digital Evolution Index 2017, проведенного компанией Mastercard совместно со Школой права и дипломатии им. Флетчера при университете Тафтса, у России есть неплохие перспективы занять лидирующие позиции в рейтинге развития цифровой экономики. По мнению экспертов, наша страна демонстрируют устойчивые темпы роста и находится на пике цифрового развития, привлекая тем самым инвесторов в экономику.

На заседании Совета по стратегическому развитию и приоритетным проектам 5 июля 2017 года президент Российской Федерации В.В. Путин заявил, что «цифровая экономика – это не отдельная отрасль, по сути это уклад жизни, новая основа для развития системы государственного управления, экономики, бизнеса, социальной сферы, всего общества».

Распоряжением Правительства Российской Федерации от 28.07.2017г. № 1632-р была утверждена программа «Цифровая экономика Российской Федерации». В Программе было выделено 5 базовых направлений развития цифровой экономики в Российской Федерации на период до 2024 года, для которых в конце 2017 года – начале 2018 года были утверждены «дорожные карты». К базовым направлениям относятся «Нормативное регулирование», «Кадры и образование», «Формирование исследовательских компетенций и технических заделов», «Информационная инфраструктура» и «Информационная безопасность». Согласно майским указам президента Российской Федерации В.В. Путина, программа «Цифровая экономика» была трансформирована в национальную программу, а ее направления стали федеральными проектами.

Очевидно, что в цифровую эпоху образование не может оставаться прежним. Закономерно, что образование вошло в один из федеральных проектов национальной программы «Цифровая экономика».

Система образования, через которую проходят все граждане нашей страны, чутко реагирует на социальные преобразования. Цифровые технологии уже пришли в образование, в том числе в систему общего образования – использование компьютера стало повседневным делом практически для всех школьников и учителей, подавляющее большинство знакомы и пользуются ресурсами сети Интернет, многие школы по всей Российской Федерации имеют компьютеры, доступ к интернету, практически все учителя и школьники используют в образовательной деятельности информационно-коммуникационные технологии.

Значительное развитие в последнее десятилетие получили дистанционные образовательные технологии. На заседании Госсовета 23 декабря 2015 года президент Российской Федерации В.В. Путин подчеркнул необходимость «в полной мере использовать преимущество информационных технологий и дистанционного обучения» и поддержал предложение рабочей группы Госсовета о создании общедоступной электронной школы для каждого школьника страны.

Трендом последних лет является развитие электронного обучения. Успешно функционирует Московская электронная школа (МЭШ) – проект, направленный на создание высокотехнологичной образовательной среды в школах города Москвы. Главная цель проекта – максимально эффективное использование современной ИТ-инфраструктуры для улучшения качества школьного образования.

Проект МЭШ получил позитивную оценку министра образования Российской Федерации О.Ю. Васильевой, и на его базе с 2016 года активно развивается Российская электронная школа (РЭШ) – открытый информационно-образовательный портал, ориентированный, прежде всего, на помощь в работе учителям и повышение доступности и качества образования на территории Российской Федерации.

Российская электронная школа содействует решению задачи выстраивания единого образовательного пространства на территории Российской Федерации, о значимости которой говорили и президент Российской Федерации В.В. Путин (15 июня 2017 года, «Прямая линия с Владимиром Путиным»), и министр образования Российской Федерации О.Ю. Васильева (интервью телевизионной сети RT, 27 сентября 2017 года).

На сегодняшний день процессы цифровизации в образовании неоднозначно воспринимаются научно-педагогическим и родительским сообществом: ведутся оживленные дискуссии, высказываются различные мнения, ставятся неоднозначные

вопросы. Действительно, цифровизация образования – сложный процесс, предполагающий как позитивные изменения, так и наличие потенциальных рисков. Поэтому важно выстроить четкую стратегию развития и систему управления процессами цифровизации в образовании, тогда можно реализовать в полной мере потенциал развития при минимальных рисках.

Важно понимать, что дальнейшее развитие цифровых технологий в образовании, в том числе в системе общего образования – неизбежный процесс. Ведь система общего образования, пожалуй, единственный социальный институт, который уже сегодня напрямую соприкасается с будущим через формирование личности ребенка – будущего гражданина. Цели и задачи образования лежат в будущем, а отличительная черта хорошего педагога – интуитивное «улавливание» тенденций будущего и развитие личности ребенка с опорой на это знание. Но цифровые технологии в образовании – это один из инструментов, они не должны полностью заменить инструменты, которыми традиционно пользовались педагоги, а только дополнить арсенал учителя, расширив образовательные возможности. В интервью телевизионной сети RT (27.09.2017г.) министр образования Российской Федерации О.Ю. Васильева, говоря о цифровизации образования, отметила «это глобальный проект, за которым, безусловно, будущее, но при этом я подчёркиваю – и мои коллеги в разных странах об этом неоднократно говорили, – что цифровое образование не может заменить образование классическое, так не бывает. Совмещение – да, но стопроцентной замены быть не может, … никто не собирается этого делать».

Цифровизация: нормативные правовые ресурсы.

На всероссийском научно-практическом форуме с международным участием «Цифровизация-2018» (3-5 декабря 2018 года, г. Москва) в своем выступлении ректор МГУ имени М.В. Ломоносова Садовничий В.А. отметил, что цифровая экономика на современном этапе своего развития немыслима без использования человеческого капитала и именно образование играет одну из ключевых ролей в цифровизации экономики. Одной из актуальных задач на сегодняшний день является создание правовых условий цифровизации экономики, и, в частности, цифровизации образования. Рассмотрим основные нормативные правовые документы, обеспечивающие данное направление развития в Российской Федерации.

Федеральный закон от 27.07.2006г. № 149-ФЗ «Об информации, информационных технологиях и о защите информации» (с изменениями и дополнениями).

Федеральный закон регулирует отношения, возникающие при осуществлении права на поиск, получение, передачу, производство и распространение информации; применении информационных технологий; обеспечении защиты информации.

Федеральный закон от 27.07.2006г. № 152-ФЗ «О персональных данных» (с изменениями и дополнениями).

Федеральным законом регулируются отношения, связанные с обработкой персональных данных с использованием средств автоматизации, в том числе в информационно-телекоммуникационных сетях, или без использования таких средств. Целью настоящего Федерального закона является обеспечение защиты прав и свобод человека и гражданина при обработке его персональных данных, в том числе защиты прав на неприкосновенность частной жизни, личную и семейную тайну.

Федеральный закон от 29.12.2010г. № 436-ФЗ «О защите детей от информации, причиняющей вред их здоровью и развитию» (в ред. Федеральных законов от 28.07.2012г. № 139-ФЗ; от 05.04.2013г. № 50-ФЗ; от 29.06.2013г. № 135-ФЗ; от 02.07.2013г. № 185-ФЗ; от 14.10.2014г. № 307-ФЗ; от 29.06.2015г. № 179-ФЗ; от 01.05.2017г. № 87-ФЗ; от 29.07.2018г. № 242-ФЗ; от 18.12.2018г. № 472-ФЗ).

Федеральный закон регулирует отношения, связанные с защитой детей от информации, причиняющей вред их здоровью и (или) развитию, в том числе от такой информации, содержащейся в информационной продукции.

Федеральный закон от 29.12.2012г. № 273-ФЗ «Об образовании в Российской Федерации» (с изменениями и дополнениями).

Ряд статей федерального закона можно рассматривать в контексте цифровизации образования: статья 16 «Реализация образовательных программ с применением электронного обучения и дистанционных образовательных технологий»; статья 18 «Печатные и электронные образовательные и информационные ресурсы»; статья 20 «Экспериментальная и инновационная деятельность в сфере образования»; статья 29 «Информационная открытость образовательной организации»; статья 98 «Информационные системы в системе образования».

Федеральный закон от 02.07.2013г. № 187-ФЗ «О внесении изменений в отдельные законодательные акты Российской Федерации по вопросам защиты интеллектуальных прав в информационно-телекоммуникационных сетях» (в ред. Федерального закона от 12.03.2014г. № 35-ФЗ).

Федеральный закон определяет порядок ограничения доступа к информационным ресурсам, посредством которых осуществляется распространение аудиовизуальных произведений и фонограмм с нарушением интеллектуальных прав правообладателей.

Указ Президента Российской Федерации от 01.12.2016г. № 642 «Стратегия научно-технологического развития Российской Федерации».

Стратегия определяет цель и основные задачи научно-технологического развития Российской Федерации, устанавливается принципы, приоритеты, основные направления и меры реализации государственной политики в этой области, а также ожидаемые результаты реализации настоящей Стратегии, обеспечивающие устойчивое, динамичное и сбалансированное развитие Российской Федерации на долгосрочный период.

В ближайшие 10-15 лет приоритетами научно-технологического развития Российской Федерации следует считать те направления, которые позволят получить научные и научно-технические результаты и создать технологии, являющиеся основой инновационного развития внутреннего рынка продуктов и услуг, устойчивого положения России на внешнем рынке, и обеспечат, в частности, переход к передовым цифровым, интеллектуальным производственным технологиям, роботизированным системам, новым материалам и способам конструирования, создание систем обработки больших объемов данных, машинного обучения и искусственного интеллекта; противодействие киберугрозам; связанность территории Российской Федерации за счет создания интеллектуальных транспортных и телекоммуникационных систем.

Для достижения цели научно-технологического развития Российской Федерации предлагается решить основные задачи, среди которых создание возможности для выявления талантливой молодежи и построения успешной карьеры в области науки, технологий и инноваций; формирование эффективной системы коммуникации в области науки, технологий и инноваций.

Указ Президента Российской Федерации от 05.12.2016г. № 646 «Об утверждении Доктрины информационной безопасности Российской Федерации».

Доктрина представляет собой систему официальных взглядов на обеспечение национальной безопасности Российской Федерации в информационной сфере. В Доктрине

на основе анализа основных информационных угроз и оценки состояния информационной безопасности определены стратегические цели и основные направления обеспечения информационной безопасности с учетом стратегических национальных приоритетов Российской Федерации.

Указ Президента Российской Федерации от 29.05.2017г. № 240 «Об объявлении в Российской Федерации Десятилетия детства».

План основных мероприятий, проводимых в рамках Десятилетия детства, до 2020 года был утвержден распоряжением Правительства Российской Федерации от 6 июля 2018 года № 375-р. План включает 131 позицию, структурированную по 15 разделам: «Повышение благосостояния семей с детьми», «Современная инфраструктура детства», «Обеспечение безопасности детей», «Здоровый ребёнок», «Всестороннее образование – детям», «Культурное развитие детей», «Развитие физкультуры и спорта для детей», «Безопасный детский отдых», «Доступный детский туризм», «Безопасное информационное пространство для детей», «Ребёнок и его право на семью», «Социальная защита детей-инвалидов и детей с ограниченными возможностями здоровья и их интеграция в современное общество», «Обеспечение и защита прав и интересов детей», «Качественные детские товары и продукты питания», «Организационные мероприятия». В некоторых разделах нашла отражение проблематика цифровизации.

Раздел «Всестороннее образование – детям»:

– обеспечение функционирования открытой информационно-образовательной среды «Российская электронная школа»;

– реализация мероприятий приоритетного проекта «Цифровая школа», включая меры по созданию образовательных ресурсов с использованием средств анимации.

Раздел «Безопасное информационное пространство для детей»:

– реализация плана мероприятий по реализации Концепции информационной безопасности детей на 2018 - 2020 годы (утвержден приказом Минкомсвязи России от 27 февраля 2018 г. № 88);

– реализация мероприятий, направленных на профилактику рисков и угроз для детей, связанных с использованием современных информационных технологий и информационно-телекоммуникационной сети «Интернет»;

– организация широкомасштабной работы с родителями (законными представителями) с целью разъяснения им методов обеспечения защиты детей в информационно-телекоммуникационной сети «Интернет»;

– проведение исследования влияния компьютерных технологий и электронного обучения на здоровье и качество образования обучающихся с инвалидностью и ограниченными возможностями здоровья.

Указ Президента Российской Федерации от 07.05.2018г. № 204 «О национальных целях и стратегических задачах развития Российской Федерации на период до 2024 года».

Среди целей развития Российской Федерации на период до 2024 года В.В. Путин поставил такие, как «ускорение технологического развития Российской Федерации, увеличение количества организаций, осуществляющих технологические инновации, до 50 процентов от их общего числа», «обеспечение ускоренного внедрения цифровых технологий в экономике и социальной сфере».

Постановление Правительства Российской Федерации от 26.10.2012г. № 1101 «О единой автоматизированной информационной системе «Единый реестр доменных имен, указателей страниц сайтов в информационно-телекоммуникационной сети «Интернет» и сетевых адресов, позволяющих идентифицировать сайты в информационно-телекоммуникационной сети «Интернет», содержащие информацию, распространение которой в Российской Федерации запрещено» (с изменениями и дополнениями от 12.10.2015г., 15.11.2016г., 21.03.2017г., 05.06.2018г.).

Постановление утверждает порядок создания, формирования и ведения единой автоматизированной информационной системы «Единый реестр доменных имён, указателей страниц сайтов сети Интернет и сетевых адресов, позволяющих идентифицировать сайты в сети Интернет, содержащие информацию, распространение которой в Российской Федерации запрещено» (единый реестр); порядок привлечения оператора реестра к формированию и ведению единого реестра; порядок принятия уполномоченными Правительством Российской Федерации федеральными органами исполнительной власти решений в отношении отдельных видов информации, распространение которой в Российской Федерации запрещено, распространяемой посредством сети Интернет.

Постановление Правительства Российской Федерации от 15.04.2014г. № 313 «Об утверждении государственной программы Российской Федерации «Информационное общество (2011 - 2020 годы)» (с изменениями и дополнениями).

Цели программы: повышение качества жизни и работы граждан, развитие экономического потенциала страны на основе использования информационных и телекоммуникационных технологий.

Цели программы:

– обеспечение качественными и доступными услугами связи, в том числе услугами по предоставлению доступа к информационно-телекоммуникационной сети «Интернет»;

– развитие информационной среды и обеспечение равного доступа граждан к медиасреде;

– предупреждение угроз, возникающих в информационном обществе;

– обеспечение предоставления гражданам и организациям государственных, муниципальных и социально значимых услуг (функций) в электронном виде.

Программа включает следующие подпрограммы (в том числе федеральные целевые программы): «Информационно-телекоммуникационная инфраструктура информационного общества и услуги, оказываемые на ее основе»; «Информационная среда»; «Безопасность в информационном обществе»; «Информационное государство»; федеральная целевая программа «Развитие телерадиовещания в Российской Федерации на 2009 - 2018 годы».

Постановление Правительства Российской Федерации от 26.12.2017г. № 1642 «Об утверждении государственной программы Российской Федерации «Развитие образования».

Программа рассчитана на 2018 - 2025 годы. Основные цели программы – качество и доступность образования, а также онлайн-образование. Программа предусматривает проектное управление. Она включает в себя реализацию таких приоритетных проектов, как «Современная цифровая образовательная среда Российской Федерации», «Вузы как центры пространства создания инноваций», «Развитие экспортного потенциала российской системы образования», «Создание современной образовательной среды для школьников», «Доступное дополнительное образование для детей», «Подготовка высококвалифицированных специалистов и рабочих кадров с учетом современных стандартов и передовых технологий».

Стратегия развития воспитания в Российской Федерации на период до 2025 года, утвержденная распоряжением Правительства Российской Федерации от 29.05.2015г. № 996-р.

Целью Стратегии является определение приоритетов государственной политики в области воспитания и социализации детей, основных направлений и механизмов развития институтов воспитания, формирования общественно-государственной системы воспитания детей в Российской Федерации, учитывающих интересы детей, актуальные потребности современного российского общества и государства, глобальные вызовы и условия развития страны в мировом сообществе.

Среди основных направлений развития воспитания в Стратегии обозначено развитие социальных институтов воспитания, которое включает в себя расширение воспитательных возможностей информационных ресурсов, а именно:

– создание условий, методов и технологий для использования возможностей информационных ресурсов, в первую очередь информационно-телекоммуникационной сети Интернет, в целях воспитания и социализации детей;

– информационное организационно-методическое оснащение воспитательной деятельности в соответствии с современными требованиями;

– содействие популяризации в информационном пространстве традиционных российских культурных, в том числе эстетических, нравственных и семейных ценностей и норм поведения;

– воспитание в детях умения совершать правильный выбор в условиях возможного негативного воздействия информационных ресурсов;

– обеспечение условий защиты детей от информации, причиняющей вред их здоровью и психическому развитию.

Концепция информационной безопасности детей, утвержденная распоряжением Правительства Российской Федерации от 02.12.2015г. № 2471-р.

В Концепции определены основные принципы обеспечения информационной безопасности детей, приоритетные задачи и механизмы реализации госполитики в этой области, ожидаемые результаты. В основу положено признание детей равноправными участниками процесса формирования информационного общества. Закреплено, что обеспечение информационной безопасности детей возможно исключительно при условии эффективного сочетания государственных и общественных усилий при определяющей роли семьи.

Среди приоритетных задач государственной политики в этой сфере названы формирование у детей навыков самостоятельного и ответственного потребления информационной продукции, повышение уровня медиаграмотности детей, воспитание у

детей уважительного отношения к интеллектуальной собственности и авторскому праву, сознательный отказ от использования «пиратского» контента.

В целях реализации Концепции был утвержден План мероприятий: приказ Минкомсвязи России от 27 февраля 2018 года № 88 «Об утверждении плана мероприятий по реализации Концепции информационной безопасности детей на 2018-2020 годы».

Распоряжение Правительства Российской Федерации от 28.07.2017г. № 1632-р «Об утверждении программы «Цифровая экономика Российской Федерации».

Программой определены цели, задачи, направления и сроки реализации основных мер государственной политики по созданию необходимых условий для развития в России цифровой экономики, что является необходимым условием повышения конкурентоспособности страны, качества жизни граждан, обеспечения экономического роста и национального суверенитета. Для управления программой были определены пять базовых направлений развития цифровой экономики в России на период до 2024 года. К базовым направлениям отнесены «Нормативное регулирование», «Кадры и образование», «Формирование исследовательских компетенций и технических заделов», «Информационная инфраструктура» и «Информационная безопасность».

Согласно майским указам президента Российской Федерации В.В. Путина (2018г.), программа «Цифровая экономика» была трансформирована в национальную программу, а ее направления стали федеральными проектами.

Цифровая компетентность.

Цифровизация образования непосредственно связана с использованием интернет-технологий. Современные технологии сети Интернет – это стремительно развивающаяся сфера с огромными перспективами, предлагающая значительный набор возможностей и функций широкому кругу потребителей.

Вовлечение обучающихся во всемирный информационный поток имеет значительные преимущества, но и несет определенные риски, что отмечается практически во всех исследованиях, посвященных проблемам использования интернет-технологий в образовательной деятельности. Так, М.Г. Васильева отмечает, что доступность интернет-коммуникаций приводит к отсутствию качественной аналитической деятельности обучающихся и студентов, которые пользуются первыми попавшимися ссылками в поисковых системах, скачивают готовые рефераты и контрольные работы. Однако, с другой стороны, интернет содержит множество полезных ресурсов, использование

которых может расширить знания[1]. Исследователь О.Е. Данилов отмечает противоречия современной образовательной деятельности: «С одной стороны, растет поток информации, которую должен воспринять учащийся. С другой стороны, учащийся часто имеет очень низкую мотивацию к усвоению этой информации»[2].

Возникает проблема правильного восприятия обучающимися информации, которое зависит от навыков аналитической работе с контентом, развития критического мышления, умения адекватно оценить достоверность информации, соотнести новую информацию с имеющимися знания, организовать информационный процесс, оценить и обеспечить информационную безопасность. И если развитию критического мышления, навыков аналитической работы традиционно уделяется много времени в процессе обучения, то формирование навыков организации информационного процесса, оценки и обеспечения информационной безопасности – это новая задача для школы. Распространение интернет-технологий ставит перед школой задачу формирования цифровой компетентности обучающихся.

Первоначально использовался термин «цифровая грамотность», который в 1997 году был популяризирован Полом Гилстером[3]. Он определил цифровую грамотность как способность критически понимать и использовать информацию, получаемую посредством компьютера в различных форматах из широкого диапазона источников. Это определение было конкретизировано Алланом Мартином, который под цифровой грамотностью понимал осознание, установки и способность отдельных лиц надлежащим образом использовать цифровые инструменты и средства для идентификации, доступа, управления, интеграции, оценки, анализа и синтеза цифровых ресурсов; построения систем новых знаний, а также общения с другими людьми с целью конструктивных социальных действий в контексте конкретных жизненных ситуаций[4].

Расширение представлений о цифровой грамотности привело к распространению понятия *«цифровая компетентность».* Анализ существующих определений показывает, что концепция цифровой компетентности относится к числу активно развивающихся, в нее постоянно вносятся изменения в соответствии с развитием современных информационно-коммуникационных технологий. Большинство авторов включает в понятие цифровой компетентности способности и навыки эффективно использовать цифровые технологии в повседневной жизни, способности и навыки критического

[1] Васильева М.Г. Интернет-ресурсы в физкультурном образовании / М.Г. Васильева // Физкультурное образование Сибири: научно-методический журнал. – № 2. – Омск, 2014. С. 7–11.
[2] Данилов О.Е. Роль информационно-коммуникационных технологий в современном процессе обучения / О.Е. Данилов // Молодой ученый. – 2013. – № 12. С. 448–451.
[3] Gilster P. Digital Literacy. N.Y.: Wiley Computer Publishing, 1997.
[4] Martin A., Madigan D. (Eds.). Digital literacies for learning. - L.: Facet, 2006.

оценивания технологий, мотивацию к участию в цифровой культуре, а также технические навыки, связанные чаще всего с компьютерной грамотностью.

Исследователи Солдатова Г.У., Рассказова Е.И. определяют цифровую компетентность как «основанную на непрерывном овладении компетенциями (знания, умения, мотивация, ответственность) способность индивида уверенно, эффективно, критично и безопасно выбирать и применять инфокоммуникационные технологии в разных сферах жизнедеятельности (информационная среда, коммуникации, потребление, техносфера), а также его готовность к такой деятельности»[5]. Таким образом, цифровая компетентность предполагает не только знания, умения и навыки пользователя, но также его мотивацию и ответственность. Солдатова Г.У., Рассказова Е.И. рассматривают цифровую компетентность как составляющую социальной компетентности человека и выделяют несколько причин появления этого понятия:

1. Популярность и значительные возможности, предоставляемые сетью Интернет, вывели его за пределы специфической сферы деятельности человека. Сеть для современного человека – это целый мир, по богатству возможностей и деятельностей ничуть не уступающий миру «офлайн» и опосредствующий все сферы жизни. Так, академическая успешность начинает напрямую зависеть от цифровой «успешности» школьников. Это означает, что общее указание на знания и навыки в рамках традиционного определения цифровой грамотности требует в сложившемся социальном контексте систематизации практически бесконечного набора этих знаний и навыков.

2. Появление цифрового мира, который меняет деятельность и жизнь человека, подразумевает необходимость исследования и учета происходящих в нем социальных, политических, этических и психологических процессов. Если еще недавно обсуждение виртуальной реальности интернета как новой уникальной формы существования человека звучало оправданно, то сегодня реальность и виртуальность уже не противопоставляются. А ограничения подхода, при котором человек рассматривается просто как пользователь виртуального пространства или специалист, его поддерживающий, становятся все более очевидны. В философии и социологии эта идея получает свое развитие в представлениях о цифровой культуре и цифровом гражданстве[6].

3. Переход к понятию цифровой компетентности имеет практические основания, поскольку согласуется с изменениями в отечественной системе образования и открывает

[5] Солдатова Г.У., Рассказова Е.И. Психологические модели российских подростков и родителей. // Национальный психологический журнал. – 2014. – « 2(14). С. 27-35.
[6] Mossberger K., Tolbert C.J., McNeal R.S. Digital citizenship: The internet, society, and participation. - Cambridge, MA: MIT Press, 2008.

возможность для применения отечественных разработок социальной компетентности[7]. В контексте культурно-исторической психологии в широком социальном и психологическом смысле компетентность определяется как «знание в действии», что требует выхода за пределы анализа знаний и умений человека.

Рассматривая цифровую компетентность как сложный комплексный феномен, определяющий сегодня жизнедеятельность человека в разных сферах информационного общества, ученые выделяют в ней соответственно четыре вида компетентности:

1. Информационная и медиакомпетентность: знания, умения, мотивация и ответственность, связанные с поиском, пониманием, организацией, архивированием цифровой информации и ее критическим осмыслением, а также с созданием информационных объектов с использованием цифровых ресурсов (текстовых, изобразительных, аудио и видео).

2. Коммуникативная компетентность: знания, умения, мотивация и ответственность, необходимые для различных форм коммуникации (электронная почта, чаты, блоги, форумы, социальные сети и др.) и с различными целями.

3. Техническая компетентность: знания, умения, мотивация и ответственность, позволяющие эффективно и безопасно использовать технические и программные средства для решения различных задач, в том числе использования компьютерных сетей, облачных сервисов и т.п.

4. Потребительская компетентность: знания, умения, мотивация и ответственность, позволяющие решать с помощью цифровых устройств и интернета различные повседневные задачи, связанные с конкретными жизненными ситуациями, предполагающими удовлетворение различных потребностей[8].

Цифровая компетентность была признана одной из 8 ключевых компетенций непрерывного обучения Европейским Союзом (Европейские рекомендации о ключевых компетенциях, 2006 год)[9].

Одной из долгосрочных целей развития цифровой компетентности может стать переход от понятия цифровой компетентности к понятию цифрового гражданства, развитие цифровой свободы личности. Цифровая свобода может быть понята как расширение возможностей индивидуального выбора технологий и культурных практик в цифровом пространстве. Таким образом, конечная цель развития цифровой

[7] Социальная компетентность классного руководителя: режиссура совместных действий / под. редакцией А.Г. Асмолова, Г.У. Солдатовой. - Москва: Смысл, 2006.
[8] Цифровая компетентность подростков и родителей. Результаты всероссийского исследования / Г.У. Солдатова, Т.А. Нестик, Е.И. Рассказова, Е.Ю. Зотова. — М.: Фонд Развития Интернет, 2013. С. 144
[9] DIGCOMP: A Framework for Developping and Understanding Digital Competence in Europe.

компетентности состоит в том, чтобы дать цифровому гражданину возможность отстаивать свою индивидуальность в интернете, осознанно формировать свою идентичность, свои ценности и убеждения, конструируя в диалоге с другими людьми новую культуру цифрового мира.

Безопасное поведение в сети Интернет.

Риски интернет-среды.

Важной составляющей цифровой компетентности современного человека, и в первую очередь такого ее компонента как ответственное поведение, является адекватная оценка рисков и угроз интернета, развитие навыков защиты от интернет-угроз. Иными словами, навыки безопасного поведения в сети Интернет – значимая составляющая цифровой компетентности.

Эффективное использование всех возможностей информационно-коммуникационных технологий для обучения и самообразования возможно лишь в сочетании со стремлением минимизировать риски, которые могут нести новые технологии. Сюда можно отнести обеспечение технической безопасности пользователя, обращение к специальным службам в случае столкновения с угрозами в Интернете, понимание, чего не нужно делать в процессе онлайн-коммуникаций (вне зависимости от степени анонимности), понимание, что в Интернете, как и в реальной жизни, надо быть осторожным. Цифровая компетентность – это, в том числе, знания и умения, позволяющие взрослым и детям использовать Интернет безопасно и критично.

Цифровая эпоха принесла с собой не только огромные возможности, но и новые опасности и риски. По мнению научного сообщества, риск – это неизбежный спутник научно-технического прогресса, а отказ от риска, по сути, означает отказ от развития. Абсолютной безопасности не бывает. Всегда существует некоторый остаточный риск. Таким образом, безопасность можно трактовать как приемлемый риск, т.е. такой уровень опасности, с которым на данном этапе научного и экономического развития можно смириться.

Исследования Фонда Развития Интернет (2009–2012 гг.) позволили выявить *основные риски интернет-среды*. Классификация включает четыре типа рисков: контентные, коммуникационные, потребительские и технические. Данное условное разделение позволяет выявить наиболее распространенные типы угроз.

1. *Контентные риски* возникают в процессе использования находящихся в сети материалов (текстов, картинок, аудио- и видеофайлов, ссылок на различные ресурсы),

содержащих противозаконную, неэтичную и вредоносную информацию (насилие, агрессию, эротику или порнографию, ненавистнический контент, нецензурную лексику, информацию, разжигающую расовую ненависть, пропаганду анорексии и булимии, суицида, азартных игр, наркотических веществ и т.д.). Столкнуться с ними можно практически везде: в социальных сетях, блогах, на торрент-сайтах, персональных сайтах, видеохостингах.

2. *Коммуникационные риски* возникают в процессе общения и межличностного взаимодействия пользователей в сети. Примерами таких рисков могут быть: кибербуллинг, незаконные контакты (например, груминг, сексуальные домогательства), знакомства в сети и последующие встречи с интернет-знакомыми в реальной жизни. С коммуникационными рисками можно столкнуться при общении в чатах, онлайн-мессенджерах (ICQ, Googletalk, Skype), социальных сетях, сайтах знакомств, форумах, блогах.

3. *Потребительские риски* возникают в результате злоупотребления в интернете правами потребителя. Они включают в себя: риск приобретения товара низкого качества, различных подделок, контрафактной и фальсифицированной продукции; потерю денежных средств без приобретения товара или услуги; хищение персональной информации с целью мошенничества.

4. *Технические риски* определяются возможностями реализации угроз повреждения программного обеспечения компьютера, хранящейся на нем информации, нарушения ее конфиденциальности или хищения персональной информации посредством вредоносных программ (вирусы, «черви», «троянские кони», шпионские программы, боты и др.).

По данным всероссийского исследования (Г.У. Солдатова, Т.А. Нестик, Е.И. Рассказова, Е.Ю. Зотова, 2013г.) наиболее часто подростки сталкиваются с рисками контентного и технического типа. Среди контентных рисков наиболее распространены сексуальные изображения и информация с насилием, жестокостью или убийствами. Среди технических – вредоносные программы. Каждый четвертый подросток жаловался на взлом его аккаунта в социальной сети или электронной почте. Практически каждый третий подросток сталкивался с коммуникационными рисками, среди которых лидирует кибербуллинг – каждый четвертый подросток указал, что сталкивался с оскорблениями, унижениями или преследованием в сети. С возрастом частота столкновения детей с интернет-угрозами возрастает.

Говоря о рисках интернет-среды, следует отдельно отметить проблему чрезмерного использования интернета. Предложенный по аналогии с зависимостью от психоактивных веществ и гэмблинга, термин «интернет-зависимость», не был полностью признан в

клинических классификациях, также существенно расходятся критерии и методы диагностики этого явления. Тем не менее, высокая частота и практическая значимость данного феномена делает актуальным дальнейшую разработку понятия и выявление его структуры. В целом, квалификация той или иной пользовательской активности подростка как «чрезмерной» требует содержательного анализа социальной ситуации развития и особенностей деятельности. Одни и те же проявления могут быть свидетельством «современного образа жизни», социальным сдвигом границ нормы и патологии, а могут – признаком аддиктивного потенциала. Близкие представления хорошо иллюстрирует М.Гриффитс, описывая два случая онлайн-игры с одной и той же высокой частотой, в одном из которых игра была важным этапом жизни молодого человека, способствуя его развитию и обогащая его жизнь (круг общения и интересов) и завершилась при изменении жизненных обстоятельств; тогда как в другом случае она «лишала», жизнь человека других интересов и смыслов, приводя к нарушениям в социальных отношениях, потере семьи и работы[10].

Преодоление рисков интернет-среды.

Можно выделить два основных стратегических направления в преодолении интернет-рисков в детской и подростковой среде: создание условий безопасного использования интернет-ресурсов и формирование навыков безопасного поведения в сети Интернет.

Создание условий безопасного использования интернет-ресурсов.

К данному направлению можно отнести следующие основные формы активности:

– ограничение доступа к деструктивной информации;

– минимизация рисков, связанных с «заражением» компьютера (и других устройств, используемых для выхода в интернет) вредоносными программами.

Ограничение доступа к деструктивной информации. Сложившаяся мировая практика фильтрации контента в сети Интернет разнообразна по формам её применения. Так, в Саудовской Аравии эта система описана на официальном сайте и содержит объяснения, почему блокируется тот или иной материал. В Китае принята политика скрытой фильтрации, применение обычно маскируется как техническая ошибка. Во Франции закрывается доступ к сайтам, которые могут способствовать разжиганию межэтнической и религиозной розни.

[10] Griffiths M. The role of context in online gaming excess and addiction: some case study evidence // International Journ. of Mental Health and Addiction. - 2010. - № 8. P. 119-125.

Известны три основные модели блокирования доступа к сайтам: сетевое, инфраструктурное и блокирование подключения пользователя. Аналитики отмечают, что по параметрам быстроты, затрат на реализацию, минимальности негативных последствий наиболее оптимально блокирование по URL с предварительным выделением запросов по IP-адресам.

Часто блокирование контента, который может представлять угрозу личности, имеет запаздывающий характер. Сайт с деструктивным содержанием должен просуществовать некоторое время и быть посещаемым, после чего он будет признан как опасный в информационном плане.

Сайтами, содержащими вредоносную информацию для несовершеннолетних лиц, признаются интернет-ресурсы, в которых допускается изображение физического и психологического насилия и сексуальных действий, присутствует информация, поощряющая наркоманию, курение и алкоголизм, ведение нездорового образа жизни, суицид, участие в азартных играх и лотереях, половую распущенность, демонстрацию гипноза и паранормальных явлений, а также компьютерные игры, вызывающие агрессивность.

В статье 14 Федерального закона Российской Федерации от 29.12.2010г. № 436-ФЗ «О защите детей от информации, причиняющей вред их здоровью и развитию» сказано, что «…доступ к информации, распространяемой посредством информационно-телекоммуникационных сетей, в том числе сети интернет, в местах, доступных для детей, предоставляется…при условии применения административных и организационных мер, технических, программно-аппаратных средств защиты детей от информации, причиняющей вред их здоровью и (или) развитию».

Один из самых простых и действенных способов помешать обучающимся получить преднамеренный или случайный доступ к нежелательному контенту – использование программного обеспечения, осуществляющего принудительную фильтрацию и блокировку определенных веб-сайтов, и позволяющего пользователям получать доступ только к предварительно одобренным интернет-ресурсам. Специалисты в сфере информационно-коммуникационных технологий, методисты могут помочь определить, какие сайты должны быть заблокированы в общеобразовательных организациях, также целесообразно проводить регулярные аудиты используемых открытых образовательных интернет-ресурсов на предмет оценки их содержания с точки зрения наличия нежелательного контента и определения необходимости их дополнительной фильтрации или блокировки.

Использование специализированного программного обеспечения по фильтрации нежелательного контента и блокировки вредоносных сайтов является одним из обязательных условий формирования безопасного интернета в школе. Технические средства контентной фильтрации должны быть сконфигурированы и настроены таким образом, чтобы обеспечивать разграничение доступа пользователей к выбору и настройкам режимов работы средств контентной фильтрации и обеспечивать отсутствие возможности их несанкционированного отключения.

В настоящее время школам и другим образовательным учреждениям доступен широкий набор программных средств фильтрации и блокировки вредоносных сайтов. Российский независимый информационно-аналитический центр Anti-Malware.ru, занимающийся исследованием вредоносных программ сети Интернет и средств защиты от них, провел экспертизу программных средств, осуществляющих контентную фильтрацию и блокировку веб-сайтов, нежелательных для посещения детей. Лучшим по эффективности фильтрации на тестовой коллекции оказался KinderGate Parental Control, заблокировавший в общей сложности 98% нежелательных для детей сайтов. Совсем немного отстал от него Kaspersky Internet Security , заблокировавший 96,8%. Их уровень ложных срабатываний не превысил 0.8%.

Минимизация рисков, связанных с «заражением» компьютера вредоносными программами. Любое вредоносное программное обеспечение пользователи зачастую называют «вирусами», хотя оно на самом деле не ограничивается только вирусами. Каждый день появляется около 200 000 новых версий вредоносных программ: вирусов, троянов, червей и др. Благодаря изобретательности злоумышленников вредоносные программы настолько разнообразны и хитроумны, что в ситуации реального столкновения с ними зачастую даже осведомленные пользователи попадают в ловушку.

Как и всякое программное обеспечение, вредоносные программы непрерывно развиваются и совершенствуются. Избежать не всех, но многих неприятностей помогают специальные комплексные программы защиты от технических интернет-угроз – программы, которые мы привыкли называть термином «антивирус». Такая защита обновляется в режиме реального времени. На самом деле антивирус является лишь частью комплексного решения информационной безопасности. Его составляющие можно разделить на пять основных групп: классический антивирус, антишпион, онлайн-сканер, сетевой экран и так называемая комплексная защита.

Большинство лицензионных средств защиты предлагает как отдельные, так и комплексные решения. Существуют платные варианты (Kaspersky Lab, ES ET NOD32, DrWeb, Avast, Trend Micro и др). Однако есть и бесплатные решения, например «Microsoft

Security Essentials» и «Avast Free Antivirus». Выбор зависит от личных предпочтений, цены лицензии, возможностей программного обеспечения и т. п.

Формирование навыков безопасного поведения в сети Интернет.

При формировании безопасного поведения необходимо не только развивать стратегии и технологии преодоления рискованных, опасных ситуаций, но и уделять внимание развитию ресурсов личности, препятствующих попаданию в ситуации повышенного риска. Для воспитания у детей и подростков таких характеристик стоит избегать избыточного информирования о рисках, опасностях, мерах по их предотвращению и т.п., тематическая информация должна быть дозированной и соответствовать возрасту. Также не следует чрезмерно оберегать детей и подростков от нового опыта, нужно сосредоточить внимание на оказании компетентной поддержки, организации сопровождения процесса освоения нового опыта. Необходимо научить детей и подростков внимательно относиться к себе, критично оценивать информацию и гибко реагировать на вызовы среды.

В обсуждаемом контексте к числу основных характеристик безопасного поведения могут быть отнесены следующие:

– у человека сформированы представления об интернет-угрозах, возможностях их минимизации и преодоления;

– у человека сформированы стратегии преодоления интернет-угроз, а именно человек способен адекватно оценить степень опасности, провести «инвентаризацию» собственных внутренних и доступных внешних ресурсов, необходимых для ее преодоления, грамотно выбрать стратегию и технологию поведения, в случае необходимости привлечь носителей внешних ресурсов, самостоятельно или с доступной поддержкой осуществить необходимые действия, нести ответственность за любые (в т. ч. и негативные) последствия собственной активности;

– у человека развиты личностные ресурсы, помогающие преодолеть сложную, опасную ситуацию (ответственность, критическое мышление, стрессоустойчивость, умение попросить помощь и принять ее и т.д.);

– поведение человека не провоцирует возникновение сложных, опасных ситуаций.

Подробно рассмотрим основные характеристики безопасного поведения в интернет-пространстве.

Формирование представлений об интернет-угрозах, возможностях их минимизации и преодоления.

Управление рисками, в том числе, рисками в сети Интернет, предполагает определенный уровень осведомленности. На сегодняшний день существует значительное количество материалов, посвященных интернет-угрозам, правилам безопасного поведения в сети Интернет. Знакомство с такими материалами, усвоение правил поведения в сети, способствует формированию необходимых представлений.

Некоммерческая организация ConnectSafely (Кремниевая долина, штат Калифорния), занимающаяся обучением пользователей интернет-технологиям в сфере безопасности и конфиденциальности, предлагает ряд несложных правил, которые помогут обеспечить безопасное и конструктивное использование интернета[11].

Коммуникации.

• Будьте доброжелательны онлайн. Можно ответить отказом на любое предложение, но при этом быть корректным.

• Если Вы впервые встречаетесь с кем-то, с кем познакомились в Интернете, проведите встречу в общественном месте.

• Узнайте, куда и как можно сообщить о насилии или заблокировать любого, кто беспокоит Вас в социальных сетях.

• Не вступайте в коммуникации с тем, кто говорит, что Вы или члены Вашей семьи должны им деньги, если Вы не уверены, что это правда.

• Будьте очень осторожны, прежде чем делиться личными фотографиями с кем-либо, даже с кем-то, кому вы доверяете. Друг может стать бывшим другом, а как только изображение появится в сети, удалить его будет невозможно.

• Будьте осторожны с сарказмом и юмором. Что-то, что может быть забавным в личном общении, может быть неправильно истолковано онлайн.

Безопасность и пароли.

• Используйте надежные и уникальные пароли.

• Не нажимайте автоматически на ссылки в электронных письмах. Они могут быть поддельными и вести вас на вредоносные сайты. Введите веб-адрес самостоятельно. В случае сомнений позвоните в компанию, которая отправила Вам электронное письмо.

• Убедитесь, что Ваш телефон блокируется. Защитите свой смартфон с помощью PIN-кода (минимум 4 цифры), пароля, отпечатка пальца или другим способом.

• Не отвечайте никому, кто скажет Вам, что Ваш компьютер заражен вирусом, даже если они утверждают, что они представители Microsoft, Apple или Вашего интернет-провайдера.

Покупки, банковское дело, пожертвования и конкурсы.

[11] По материалам сайта connectsafely.org. Режим доступа: https://www.connectsafely.org/safetytips/.

• Если это звучит слишком хорошо, чтобы быть правдой, это слишком хорошо, чтобы быть правдой. Вы не можете выиграть конкурс, в котором не участвовали, и нигерийские принцы не готовы отправить Вам деньги.

• Делайте покупки только у известных, проверенных онлайн-продавцов. Если есть сомнения, поинтересуйтесь репутацией продавца.

• Никогда не отправляйте наличные деньги, используйте кредитные карты, если это возможно, в противном случае используйте дебетовые карты или законные платежные услуги (системы).

• При совершении покупок или банковских операций ищите безопасные сайты, веб-адрес которых начинается с HTTPS. «S» означает безопасный.

• Прежде чем делать пожертвования он-лайн, убедитесь, что благотворительность законна, и что деньги идут на благое дело.

• Никогда не сообщайте номер своего полиса социального страхования, полиса медицинского страхования или любого удостоверения личности, если не уверены, что это требование законно.

Использование приложений и неизвестных сайтов.

• Читайте отзывы перед загрузкой приложений для смартфонов.

• Обратите внимание на то, какие разрешения запрашивают приложения для смартфонов, прежде чем загружать или использовать их.

• Узнайте и используйте настройки конфиденциальности для любого устройства, приложения или услуги, которыми Вы пользуетесь.

• Не предоставляйте личную информацию на веб-сайте, если не уверены, что это законно. И даже если это законно, делайте так, только если это необходимо.

Советы по безопасности в социальных сетях.

• Научитесь пользоваться настройками конфиденциальности каждой службы или приложения.

• Не позволяйте друзьям или незнакомцам оказывать на Вас давление. Знайте свои возможности. Возможно, Вы разбираетесь в интернете, но люди и отношения меняются, и в интернете могут происходить неожиданные вещи.

• Будьте доброжелательны в интернете и относитесь к людям так, как Вы бы хотели, чтобы относились к Вам. Люди, проявляющие агрессию в интернете, подвергаются большему риску запугивания или преследования. Если кто-то ведет себя агрессивно по отношению к Вам, постарайтесь не реагировать, не мстите. Используйте инструменты конфиденциальности, чтобы заблокировать недоброжелателей.

• Подумайте о том, что Вы публикуете. Отправка провокационных фотографий или интимных подробностей в интернете, даже в личных электронных письмах, может впоследствии вызвать проблемы. Даже люди, которых Вы считаете друзьями, могут использовать эту информацию против Вас, особенно в случае ссоры. Аккаунты Ваших друзей могут взломать, их устройство могут украсть, или они могут случайно переслать то, что Вы им отправили.

• Читайте между строк. Имейте в виду, что некоторые люди могут предлагать Вам свою дружбу, чтобы что-то получить. Лесть или поддерживающие сообщения могут быть просто манипуляцией, а не дружбой или романтическими отношениями.

• Избегайте личных встреч. Единственный способ, которым кто-то может причинить Вам физический вред, – это если вы оба находитесь в одном месте, поэтому, чтобы быть в полной безопасности, не встречайтесь лично. Если Вам действительно нужно встретиться с кем-то, кого Вы «встретили» в интернете, не ходите в одиночку. Проведите встречу в общественном месте, сообщите родителям или другим надежным помощникам, приведите с собой друзей.

Медиаграмотность и фальшивые новости.

• Помните, что не все, что Вы читаете в интернете, обязательно является правдой.

• Подумайте об источнике информации, и, если у Вас есть какие-либо сомнения, проведите небольшое онлайн-исследование, чтобы убедиться в правдивости информации.

• Никогда не делитесь чем-то, в чем у Вас есть основания сомневаться. Делиться недостоверной информацией не только плохо, но и подрывает Ваш авторитет.

• Помните, не вся информация, которая вызывает у Вас эмоциональный отклик и кажется Вам правильной, правдива.

Кибербуллинг: советы для детей и подростков.

• Знайте, что это не Ваша вина. Если кто-то постоянно жесток с Вами, это издевательство, и Вы не должны винить себя. Никто не заслуживает жестокого обращения.

• Не отвечайте и не мстите. Иногда реакция – это именно то, что ищут агрессоры, потому что они думают, что это дает им власть над Вами, а мы не хотим придавать силы хулигану. Что касается ответного удара, то он может поставить Вас на один уровень с хулиганом, одно подлое действие может превратиться в цепную реакцию. Если можете, «выключитесь» из ситуации. Если не можете, иногда юмор обезоруживает или отвлекает человека от издевательств.

• Сохраните доказательства. Единственная хорошая новость об издевательствах в интернете или в телефоне заключается в том, что доказательства обычно можно сохранить

и показать тому, кто может помочь. Вы можете сохранить эти доказательства на случай, если ситуация обострится.

• Попросите человека остановиться. Это полностью зависит от Вас, Вам нужно четко заявить о своей позиции, что Вы больше не будете терпеть такое обращение. Возможно, Вам придется заранее потренироваться с кем-то, кому Вы доверяете, например, с родителем или хорошим другом.

• Обратитесь за помощью, особенно, если агрессивное поведение действительно травмирует Вас. Вы заслуживаете поддержки. Посмотрите, есть ли кто-то, кто может выслушать, помочь разобраться в происходящем – друг, родственник или, может быть, взрослый, которому Вы доверяете.

• Используйте доступные технические инструменты. Большинство приложений и сервисов социальных сетей позволяют блокировать человека. Будь то преследование в приложении, текстовые сообщения, комментарии или фотографии с тегами, сделайте себе одолжение и заблокируйте человека. Вы также можете сообщить о проблеме в службу поддержки. Если Вы получаете угрозы физической расправы, Вы должны обратиться в полицию (с помощью родителей или опекуна).

• Защитите свои учетные записи. Не делитесь своими паролями с кем-либо, даже с самыми близкими друзьями, защищайте свой телефон паролем, чтобы никто не мог воспользоваться им и выдать себя за Вас.

• Если над кем-то из Ваших знакомых издеваются, примите меры. Лучшее, что Вы можете сделать, это попытаться остановить издевательства, выступая против него. Если Вы не можете остановить это, поддержите человека, над которым издеваются. Если Ваш друг подвергся издевательствам, Вы можете выслушать его и подумать, как можно помочь. Подумайте вместе, стоит ли сообщать о запугивании. Если это просто знакомый, даже доброе слово может помочь и утешить человека. Можно помочь, не поддерживая и осуждая человека, совершающего издевательства.

Использование телефона (смартфона).

• Телефон – это предмет для личного пользования. Позволять другим людям использовать Ваш телефон, когда Вас нет рядом, это все равно, что дать им пароль к Вашему профилю в социальной сети. Они могут выдать себя за Вас, что дает им возможность испортить Вашу репутацию и отношения. Блокируйте телефон, когда Вы его не используете, и используйте надежные и уникальные пароли для всех Ваших приложений.

• Просматривайте свои фотографии, чтобы убедиться, что они уместны. Подумайте о том, как Вы и другие одеты, подумайте, вдруг что-то на заднем плане может смутить

Вас или лишить Вас конфиденциальности. Узнайте, как отключить совместное использование фотографий, уважать частную жизнь других людей, не публикуя их фотографии без разрешения.

• Ценность присутствия. Если Вы постоянно «сидите в телефоне», подумайте, какое впечатление Вы производите на других людей, насколько им приятно такое Ваше поведение во время общения: во время еды, на вечеринках, в машине и т.д. Чрезмерное увлечение телефоном – признак невежливости, дурного воспитания.

• Обратите внимание на то, что «знают» ваши приложения. Обратите внимание на любые запросы разрешений приложений при их установке. Если приложение запрашивает доступ к вашему местоположению, списку контактов, календарю, сообщениям или для публикации в социальных сетях, подумайте, действительно ли приложению нужна эта информация для работы. В случае сомнений рассмотрите возможность удержания разрешения или не использования этого приложения.

• Иногда отдыхайте от телефона. Постоянная переписка и разговоры могут повлиять на сон, концентрацию, учебу и другие вещи, которые заслуживают Вашего внимания. Настоящие друзья с пониманием отнесутся к тому, что иногда Вам просто нужно выключить телефон.

• Растет число приложений, позволяющих друзьям точно определять местонахождение друг друга. Если Вы используете такой сервис, делайте это только с друзьями, которых Вы знаете лично, и узнайте о функциях конфиденциальности сервиса.

• Поговорите со своими детьми об использовании смартфона. Подумайте о том, чтобы составить контракт на семейный мобильный телефон и поговорите со своими детьми о том, почему это важно. Если Вы решили использовать приложения для родительского контроля, обсудите их со своими детьми.

• Рассмотрим инструменты родительского контроля. Существует два основных типа родительского контроля. Первый – это семейные правила или руководящие принципы, которые Вы устанавливаете со своими детьми, а второй – технологические инструменты, предоставляемые компаниями по производству мобильных телефонов, производителями смартфонов и разработчиками приложений. Если Вы используете технологию для отслеживания или ограничения телефонных операций Вашего ребенка, в большинстве случаев полезно заранее поговорить с ними и периодически пересматривать их по мере взросления детей.

• Не отвлекайтесь на телефон во время вождения, это опасно. Если Вам нужно поговорить по телефону, используйте гарнитуру или устройство громкой связи. Никогда не отправляйте текстовые сообщения, не отправляйте и не читайте электронные письма,

не размещайте сообщения в соцсетях, находясь за рулем. Если Вы пользуетесь телефоном для навигации или прослушивания музыки, настройте его перед началом движения или используйте функцию дистанционного управления телефоном (например, при помощи голоса).

Стратегии преодоления интернет-угроз и развитие личностных ресурсов.

В строящемся информационном обществе функции социализации детей и подростков начинает активно брать на себя интернет. Как и в реальном мире, в виртуальном дети и подростки встречаются с различными трудностями, кризисными ситуациями, причем большинство жизненных стрессовых ситуаций в той или иной форме можно встретить в интернете. Например, как в реальной, так и в виртуальной жизни пользователей случаются конфликты, можно столкнуться с непониманием, агрессией, домогательствами, мошенничеством, кражами, проявлениями экстремизма и .т.д.

Столкновение с трудными ситуациями в интернет-пространстве (с интернет-рисками) вызывает у детей и подростков стресс различной степени выраженности. Сила стресса во многом зависит от индивидуальных особенностей личности пользователя. Если ребенок, подросток в реальной жизни эмоционально реагирует на сложные и проблемные ситуации, то есть большая вероятность того, что, сталкиваясь в интернете с негативными ситуациями, например, с оскорблением и унижением, насилием, жестокостью, сексуальными домогательствами и пр., он будет также испытывать высокий уровень стресса.

Сегодня при трактовке «трудных» ситуаций исследователи выделяют их значимость для человека и воспринимаемую трудность[12]. Субъективная оценка ребенком ситуации столкновения с онлайн-рисками как расстраивающей, рассматривается в качестве показателя того, что данная ситуация переживается им как «трудная», следовательно, требующая преодоления. Для преодоления трудной жизненной ситуации, в том числе трудностей, встречающихся в интернет-пространстве, человек использует личностные ресурсы и стратегии поведения. Формирование стратегий совладания (преодоления) происходит во взаимодействии личности и трудной ситуации.

Индивидуальные способы взаимодействия с трудной (внешней или внутренней) ситуацией, которые определяются ее субъективной значимостью для человека и его

[12] Marriage K., Cummins R.A. Subjective quality of life and self-esteem in children: the role of primary and secondary control in coping with everyday stress // Social Indicators Research. - 2004. - Vol. 66. - N 1-2. P. 107-122.

собственными психологическими ресурсами, называют «копингами»[13]. Поведение, направленное на преодоление стрессовых состояний – т.е. на изменение или разрешение критической ситуации, либо привыкание к ней, или уклонение от требований, которые она предъявляет – называют копинг-поведением (от англ. coping – совладание, преодоление).

В процессе развития ребенка освоение копинг-поведения идет параллельно с развитием психологических личностных ресурсов (качественных изменений когнитивной сферы, преобразования социальных связях, формирования представления о себе и др.). Психологические ресурсы личности являются основой копинга[14].

Из всего многообразия копинг-стратегий остановимся на наиболее важных, с точки зрения российских исследователей (Солдатова Г.У., Рассказова Е.И.) для преодоления интернет-рисков.

Проактивные (активные) стратегии совладания: предполагают активное преодоление ситуации, включающее поиск и пробы новых форм поведения (например, изменение настроек безопасности, блокирование агрессора, попытка отомстить агрессору и др.). Проактивное совладание ориентировано на видение возможностей мира и потенциальное развитие, направлено на постановку и достижение новых целей и личностный рост.

Реактивные (пассивные) стратегии совладания: стратегии избегания, в отличие от активных стратегий характеризуются игнорированием стрессоров, уходом от проблем (например, временное прекращение пользования интернетом, удаление агрессивных сообщений, надежда, что проблема разрешится сама собой и др.).

По мере взросления школьники чаще отдают предпочтение активным стратегиям. Это может означать, что они все лучше осваивают онлайн-пространство и выстраивают свою онлайн-среду, в которой функционируют и взаимодействуют с другими пользователями[15].

Копинг по типу поиска социальной поддержки: важнейшим ресурсом совладания с трудными жизненными ситуациями, особенно в контексте деятельности ребенка, подростка в интернете, являются значимые другие. Поиск «значимых других» при совладании с трудными онлайн-ситуациями смещается в пространство интернета, дети все

---

[13] Белинская Е.П. Совладание как социально-психологическая проблема / Е.П. Белинская. - Психологические исследования: электронный научный журнал. - 2009. - № 1(3). - Электронный ресурс. - Режим доступа: http://psystudy.ru.

[14] Никольская И.М., Грановская Р.М. Психологическая защита у детей. - СПб.: Речь, 2006. С. 342

[15] Subrahmanyam K., Smahel D. Digital Youth, Advancing Responsible Adolescent Development, Springer Science+Business Media, LLC, 2011.

реже обращаются к родителям, предпочитая им в роли значимых других друзей и компетентных людей в онлайн-среде.

Собственная активность ребенка, подростка в интернете, попытки преодолеть сложную ситуацию, поиски решения важны не только для преодоления стресса и его негативных последствий, но и для дальнейшего развития личности в цифровом мире, определения собственной позиции по отношению к произошедшему, развития цифровой компетентности.

Поведение, провоцирующее возникновение опасных онлайн-ситуаций.

Подростки склонны к риску и стремятся выйти за пределы дозволенного, что может повлиять на формирование деструктивного поведения в интернет-пространстве.

Подростки могут стать источником интернет-угроз как намеренно, так и неосознанно, случайно. Сознательно подросток может стать автором и распространителем неэтичной, противозаконной информации (насилие, агрессия, ненавистнический контент, нецензурная лексика и т.п.), стать инициатором или участником кибербуллинга, или даже создавать и распространять вредоносное программное обеспечение. Не задумываясь об этике и последствиях своего поведения, подросток может, например, загружать нелицензионные программы, нарушать авторские права, пользуясь «пиратским» контентом, репостить неподобающую или даже незаконную информацию.

Основной стратегией предотвращения поведения, провоцирующего возникновение опасных онлайн-ситуаций, является формирование у подростков ответственности за собственные поступки. В этой связи важно обсудить:

– этические нормы поведения в интернет-пространстве (сетевой этикет);

– деятельность в сети, которая является противозаконной (например, распространение информации экстремистской направленности, демонстрация запрещенной символики, разжигание межнациональной и межрелигиозной вражды, участие в сетевых азартных играх (онлайн-казино) и др.);

– личную ответственность подростка при пользовании интернетом.

В заключении сформулируем *основные навыки безопасного поведения в сети Интернет*, которыми должен обладать ребенок, подросток:

– использовать нормы сетевого этикета и действующего законодательства в собственной интернет-активности;

– оберегать личные данные, защищать свои учетные записи, пользоваться настройками конфиденциальности;

– уметь анализировать степень достоверности информации и подлинность ее источников;

– критически относиться к информации, распространяемой в интернете, по смс и через другие каналы коммуникации;

– избегать информации, которая способна причинить вред здоровью, нравственному и психическому развитию, чести, достоинству и репутации;

– распознавать манипулятивные техники, используемые в рекламе и иной информации;

– применять эффективные меры защиты от нежелательных контактов в интернете;

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

– избегать «заражения» компьютера (и других устройств, имеющих доступ к сети Интернет) вредоносным программным обеспечением;

– уметь использовать ресурсы социальной поддержки (т.е. в сложных ситуациях уметь обратиться за помощью к взрослым).

Обеспечение безопасности детей и подростков в сети Интернет.

Позитивный опыт европейских стран показывает, что лучшее средство обеспечить безопасность несовершеннолетних в интернет-пространстве – коллективные действия и коллективная ответственность всех заинтересованных субъектов: государства, образовательных организаций, родителей, общественных и коммерческих организаций. Ответственность за формирование безопасного поведения детей и подростков в сети Интернет и обеспечение информационной безопасности в равной степени должны разделить государство, образовательные организации и родители. Приоритетом в обеспечении безопасности несовершеннолетних в интернет-пространстве должно стать повышение уровня цифровой компетентности, как самих детей и подростков, так и педагогов и родителей.

Сфера ответственности государства.

① Создание нормативно-правовой базы.

Обеспечение государством информационной безопасности детей, защита физического, умственного и нравственного развития несовершеннолетних, а также охрана человеческого достоинства во всех текстовых и аудиовизуальных сетевых медиа-средах, из которых состоит современный интернет, является требованием международного права.

Международные стандарты в области информационной безопасности детей нашли свое отражение и в российском законодательстве.

② Обеспечение соблюдения действующего законодательства.

Помимо разработки законодательной базы в области информационной безопасности граждан, на уровне государственного регулирования должно быть обеспечено строгое соблюдение действующего законодательства. При этом кибер-безопасности детей уделяется особое внимание, в 2010 году был принят Федеральный закон «О защите детей от информации, причиняющей вред их здоровью и развитию» (от 29.12.2010г. № 436-ФЗ), механизмы соблюдения которого хорошо проработаны и действуют. Конкретная деятельность государства в обеспечении безопасного интернета для детей и подростков проявляется, в первую очередь, в контроле над имеющимся в сети контентом в соответствии с действующим законодательством и применении средств фильтрации контента и блокировки веб-сайтов, несущих вред детскому сознанию.

③ Инициирование и поддержка просветительских проектов.

Органы государственного управления, часто совместно с общественными или коммерческими организациями, инициируют и развивают просветительские проекты, например, составление и распространение «черных списков» интернет-ресурсов, несущих кибер-угрозы. Целям информационной безопасности служат телефонные «горячие линии», поддерживаемые либо финансируемые государством, и информирующие о противоправных действиях, выявленных в сети интернет, а также о способах нейтрализации и борьбы с ними.

④ Развитие единого образовательного пространства.

Единое образовательное пространство России – это в первую очередь единство возможностей доступа к качественному и вариативному образованию. Ключевыми инструментами формирования единства образовательного пространства в нашей стране являются федеральные государственные образовательные стандарты. В действующих стандартах на разных уровнях образования важное место занимают вопросы формирования цифровой компетентности и информационной безопасности детей, подростков и молодежи. Примером развивающегося проекта, содействующего выстраиванию единого образовательного пространства на территории Российской Федерации, является Российская электронная школа (РЭШ).

Сфера ответственности родителей.

① Повышение уровня собственной цифровой компетентности.

Дети, подростки и молодежь постигают технологические новинки на лету, естественно и без напряжения. Взрослые в силу занятости и уже привычных схем поведения не всегда за ними поспевают. Поэтому дети чаще, чем взрослые, глубже погружены в цифровой мир и обладают более разнообразными навыками в онлайн-пространстве.

По данным российского исследования[16] многие родители ощущают необходимость большего участия в «сетевой» жизни ребенка, но для этого у них недостаточно знаний и умений. Большинство родителей ждут поддержки со стороны школы, государства и интернет-индустрии: более половины всех опрошенных родителей полагают, что за безопасность в интернете ответственны школа, государство или интернет-индустрия. Вместе с тем лишь небольшое число родителей считает, что ситуацию могут улучшить инфокампании, специализированные сайты или службы помощи. И только каждый четвертый родитель считает обеспечение безопасности ребенка в интернете своей ответственностью.

② Медиация родителей.

Под медиацией в контексте системы «ребенок – интернет» понимаются любые виды посредничества и поддержки пользовательской онлайн деятельности детей и подростков. Изучение родительской медиации стало одной из задач масштабного европейского проекта EU Kids Online, в рамках исследования было выделено пять основных типов медиации родителей[17]:

1. Активная медиация использования интернета – родитель присутствует при использовании интернета ребенком и помогает ему.

2. Активная медиация безопасности ребенка в интернете – родитель общается с ребенком о том, как безопасно вести себя в интернете, дает советы и учит, как правильно себя вести.

3. Ограничивающая медиация – родитель создает правила и ограничения пользования интернетом.

4. Мониторинг – постоянная проверка сайтов, которые посещает ребенок, его контактов, сообщений, профилей.

5. Техническое ограничение – использование специальных программ, которые позволяют блокировать и фильтровать сайты, отслеживать посещенные сайты или устанавливать ограничения на время пользования.

---

[16] Цифровая компетентность подростков и родителей. Результаты всероссийского исследования / Г.У. Солдатова, Т.А. Нестик, Е.И. Рассказова, Е.Ю. Зотова. – М.: Фонд Развития Интернет, 2013. С. 144.

[17] Livingstone, S., Haddon, L., Görzig, A., & Ólafsson, K. (2011a). Risks and safety on the internet: The perspective of European children. Full findings. London: EU Kids Online, LSE.

Результаты исследования российских ученых[16] свидетельствуют об особенностях стратегий медиации, применяемых российскими родителями, по сравнению с европейскими родителями. Из-за цифрового разрыва и недооценки существующих рисков родители практически не используют технические средства для контроля того, что ребенок делает в интернете. Статистический анализ позволил выделить три надежных шкалы оценки родительских стратегий: запреты и ограничения, мониторинг, объяснения и поощрения.

Сфера ответственности образовательных организаций.

① Формирование цифровой компетентности обучающихся.

Интернет находится в процессе постоянного развития, высокий темп технологических изменений рассматривается как важное измерение информационного общества. По данным исследований Фонда Развития Интернет 75 % подростков овладевали цифровыми компетенциями самостоятельно, получали знания об интернете «на ощупь», идя путем проб и ошибок. Подростки самостоятельно научились искать в интернете информацию и завязывать знакомства, но наедине с сетью им гораздо труднее критически оценивать найденное, освоить создание своего контента и взаимодействие с интернет-сообществами.

Целенаправленное развитие цифровой компетентности детей и подростков должно изменить эту ситуацию, запуская виртуальные исследовательские проекты, делая освоение и преобразование интернета школьниками коллективным проектом, вовлекающим все заинтересованные стороны: родителей, педагогов, представителей профессионального интернет-сообщества.

Сегодня мы наблюдаем дуальную ситуацию. С одной стороны, дети выражают общую готовность учиться, высказывают заинтересованность в повышении своей цифровой компетентности: каждый второй подросток указал в числе наиболее предпочитаемых форм обучения – обучение с использованием информационно-коммуникационных технологий, интернета, а в числе полезных курсов – получение систематической информации о новинках и изменениях в этой области. Вместе с тем часто интерес не переходит в поле активной деятельности. Это связано с иллюзией достаточной цифровой компетентности – ошибочного впечатления, что ничего больше знать и уметь не нужно. Но технологии развиваются молниеносно, и как бы ни были хороши знания и умения подростка в цифровой среде, если он не хочет и не считает нужным учиться дальше, он неизбежно отстанет.

Одной из ключевых составляющих цифровой компетентности, помимо освоения новых информационных технологий, оценки их возможностей и рисков, должна быть готовность ребенка, подростка к восприятию возрастающего темпа изменений, обучающих программах по повышению цифровой компетентности важно формировать установку на постоянное обновление знаний и приобретение новых компетенций.

② Обеспечение информационной безопасности обучающихся.

Понимание рисков, обусловленных развитием современных информационно-коммуникационных технологий, требует от педагогов и обучающихся формирования социально ответственного отношения к своей деятельности в сети интернет. На педагогов налагаются дополнительные обязательства по взаимодействию с детьми, подростками с целью снижения таких риски и предотвращению возможного будущего ущерба. Этот вид социальной ответственности является важнейшей составляющей цифровой компетентности.

③ Повышение уровня цифровой компетентности педагогов.

Известный российский ученый и психолог А.Г. Асмолов считает, что развитие способности к обучению ученика начинается с развития способности к обучению учителя[18].

Очевидно, что необходимое условие создания новой школы – педагоги, обладающие цифровой компетентностью и умело использующие эти компетенции для формирования как академической, так и цифровой компетентности обучающихся.

Исследования показывают, что по сравнению со своими учениками, педагоги, так же как и взрослые в целом, менее вовлечены в жизнь онлайн. Только половину педагогов можно отнести к категории активных интернет-пользователей, около трети опрошенных составляют группу умеренных пользователей (заходят в интернет не чаще одного или двух раз в неделю), третья группа – примерно десятая часть выборки – это случайные пользователи, которые не испытывают особой потребности в интернете как постоянном источнике информации или как средстве общения, и посещали сеть исключительно по необходимости. Следует отметить, что интернет-активность педагогов зависит от возраста: в среднем, молодые педагоги чаще являются активными пользователями.

④ Активное использование информационно-коммуникационных технологий в обучении.

В настоящее время все мы присутствуем при рождении принципиально новых образовательных систем, основанных на последовательном,

[18] Асмолов А.Г. Оптика просвещения: социокультурные перспективы. — М.: «Просвещение», 2012. С. 447.

всеохватывающем использовании компьютерных и сетевых технологий. Уже сегодня дети, подростки и молодые люди получают большую часть своих знаний, совершенствуют свои компетенции именно в сети Интернет.

Эффективное использование всех возможностей информационно-коммуникационных технологий для обучения и самообразования возможно лишь в сочетании со стремлением минимизировать риски, которые могут нести новые технологии. Сюда входит обеспечение технической безопасности, обращение к специальным службам в случае столкновения с интернет-угрозами, понимание, чего не нужно делать в процессе онлайн-коммуникаций (вне зависимости от степени анонимности), что в сети Интернет, как и в реальной жизни, надо быть осторожным. Цифровая компетентность – это, в том числе, знания и навыки, позволяющие использовать Интернет безопасно и критично.

⑤ Просветительская деятельность.

Важным направлением деятельности общеобразовательной организации является педагогическое и социальное взаимодействие с семьями обучающихся. В соответствии с положениями Федерального закона от 29.12.2012г. № 273-ФЗ «Об образовании в Российской Федерации» родитель является полноправным субъектом образования своего ребёнка, имеющим «преимущественное право на обучение и воспитание детей перед всеми другими лицами». Закон определил в качестве одной из компетенций общеобразовательных организаций оказание помощи родителям в воспитании ребенка, охране и укреплении его физического и психического здоровья, развитии индивидуальности, присущих только ему способностей, коррекций нарушения их развития, на это указывают и федеральные государственные образовательные стандарты.

В качестве цели педагогического просвещения родителей в контексте формирования цифровой компетентности предполагается наделение их некоторым минимумом знаний, оказание необходимой помощи в самообразовании, формировании навыков компетентного и безопасного сетевого поведения, мотивация на выстраивание взаимодействия с детьми в сфере информационно-коммуникационных технологий.

Просветительская деятельность в отношении родителей в сфере цифровой грамотности может осуществляться через коллективные формы работы (лекции, беседы, практикумы, диспуты, конференции) и индивидуальные (индивидуальные консультации и беседы). Задачей каждой общеобразовательной организации, каждого педагога является выбор наиболее подходящих форм просвещения, удобных для школы и интересных для родителей (школьные лектории, общешкольные и классные конференции на интересующие родителей темы, индивидуальные консультации, обзоры и выставки

соответствующей литературы и программных средств, совместная деятельность педагогов, родителей и детей и др.).

ПРАКТИЧЕСКИЕ РЕКОМЕНДАЦИИ ПО ФОРМИРОВАНИЮ У ОБУЧАЮЩИХСЯ НАВЫКОВ БЕЗОПАСНОГО ПОВЕДЕНИЯ В СЕТИ ИНТЕРНЕТ

Научно-методическим основанием практических рекомендаций по формированию у обучающихся навыков безопасного поведения в сети Интернет являются описанные в первой части настоящих методических рекомендаций теоретические аспекты проблематики: анализ действующей нормативно-правовой базы цифровизации экономики, понимание процессов цифровизации образования, особенности формирования цифровой компетентности детей и подростков в целом и, как важнейшая ее составляющая, формирование безопасного поведения в сетевом пространстве.

Практические рекомендации ориентированы на оказание методической помощи педагогам в организации и проведении тематических занятий по развитию у обучающихся навыков безопасного сетевого поведения. Практические рекомендации по формированию у обучающихся навыков безопасного поведения в сети Интернет структурированы по уровням общего образования, а также включают раздел, посвященный полезным тематическим информационным ресурсам.

Образовательная деятельность по формированию у обучающихся навыков безопасного поведения в сети Интернет.

Занятия по формированию навыков безопасного поведения в сети Интернет могут быть реализованы в рамках основной образовательной программы через урочную и внеурочную деятельность, в системе дополнительного образования (кружки, клубы и т.д.), в учреждениях культурно-досуговой сферы (занятия просветительской направленности в библиотеках, досуговых центрах, тематические выставки и т.д.).

Форма организации образовательной деятельности.

Тематические занятия по формированию навыков безопасного поведения в сети Интернет могут различаться по форме организации, в качестве основных мы рекомендуем рассмотреть следующие: традиционное занятие (урок) комбинированного типа, занятие-беседа, занятие-дискуссия (диспут), практическое занятие, занятие-путешествие, занятие-сказка, занятие-конференция, занятие-«клуб знатоков» (экспертный совет), встреча с профильным специалистом.

Любое занятие должно органически вписываться в систему работы учителя. При выборе формы организации занятия следует ориентироваться на возрастные и психофизиологические особенности обучающихся, имеющиеся ресурсы. Занятие должно отличаться целостностью и завершенностью, выполнять конкретные задачи и достигать поставленных результатов. Как традиционное (классическое), так и нетрадиционное по форме занятие должно являться конкретным воплощением определенной методической концепции.

Методы и приемы организации образовательной деятельности.

При проведении тематических занятий по формированию навыков безопасного сетевого поведения можно использовать различные методы и приемы организации образовательной деятельности в их оптимальном сочетании.

Под *методом обучения* мы понимаем определенным образом упорядоченную деятельность, обеспечивающую эффективное руководство педагога работой обучающихся по овладению знаниями. Целесообразность использования тех или иных методов обучения определяется его целями и содержанием. Овладение содержанием обучения во многом определяется методами, которые применяет педагог.

В ходе занятий по развитию цифровой компетентности обучающихся целесообразно отдавать предпочтение активным (презентации, кейс-технологии, дидактические игры и др.) и интерактивным (интерактивное занятие с применением аудио- и видеоматериалов, ИКТ, метод проектов, игры (деловые, сюжетно-ролевые, познавательные, вербальные), дискуссия, круглый стол, диспут, мозговой штурм и др.) методам обучения. Активные и интерактивные методы обучения призваны решать главную задачу, сформулированную в федеральных государственных образовательных стандартах – научить ребенка учиться, развивать критическое мышление, основанное на умении самостоятельно искать информацию, логически ее осмысливать, делать выводы, принимать взвешенные и аргументированные решения.

Доказано, что сочетание в рамках занятия нескольких методов обеспечивает смену видов деятельности, позволяет вовлечь в активную работу максимальное количество обучающихся, повышает эффективность образовательной деятельности.

НАЧАЛЬНОЕ ОБЩЕЕ ОБРАЗОВАНИЕ

Возрастные особенности обучающихся начальной школы в контексте развития навыков безопасного поведения в сети Интернет.

Младший школьный возраст благоприятен для формирования у детей базовых представлений о полезном и безопасном использовании интернета. Возраст 8-9 лет – период активной смены ведущей деятельности: сюжетно-ролевая игра начинает уступать место учебе, потребность в получении и усвоении новых знаний, в т. ч. по вопросам использования информационно-коммуникационных технологий, активно формируется. Именно поэтому при проведении занятия педагогу крайне важно стимулировать собственную активность участников занятия и придерживаться принципов субъект-субъектного взаимодействия, т.е. транслировать обучающимся, что они такие же равноправные участники образовательной деятельности, как и учитель.

В младшем школьном возрасте происходят качественные изменения в познавательном развитии ребенка. Центральными новообразованиями этого периода становятся словесно-логическое мышление, вербальное дискурсивное мышление, смысловая память, произвольное внимание и письменная речь. В качестве материалов к занятию должны быть подобраны задачи, которые требуют индуктивных (от частного к общему) и дедуктивных (от общего к частному) умозаключений. Для решения поставленных задач в занятии используются методы визуализации, обсуждения и интерактивной игры, способствующие развитию у обучающихся произвольного внимания и поведения, использование метода проблемных ситуаций способствует ориентировке, развитию критического мышления и интериоризации (присвоение) способов безопасного поведения в интернете.

Нельзя забывать о том, что ключевое значение в образовательной деятельности детей младшего школьного возраста приобретает мотивация. Именно поэтому занятие должно быть спроектировано таким образом, чтобы актуализировать интерес к проблемам и возможностям, возникающим при освоении цифровой среды. Школьники получают новые знания не только в готовом виде, но и в форме проблемно-поисковых задач, стимулирующих собственную познавательную активность и самостоятельный поиск новой информации по обсуждаемой теме. При этом важное место в структуре занятия играет обсуждение результатов. Благодаря критическому осмыслению информации при подведении итогов упражнений и урока в целом, а также возможности ее соотнесения с имеющимся личным опытом у школьников формируется способность к рефлексии собственной деятельности за цифровыми устройствами. Это является залогом их интернет-безопасности и способствует тому, что знания, которые школьники получают на занятии, затем с легкостью интегрируются в их повседневную деятельность.

В подавляющем большинстве случаев дети испытывают неподдельный интерес к проблемам использования интернета и активно делятся своим опытом. Обычно самыми

популярными темами обсуждений становятся поисковые системы и использование антивирусов. Дети выглядят достаточно осведомленными в этих вопросах. Тем не менее, стоит сделать особый акцент при объяснении сути программ фильтрации и родительского контроля, предложить детям попросить родителей установить эти программы на домашний компьютер или гаджеты. Также следует знать, что до сих пор встречаются дети, не имеющие опыта использования интернета. Им необходимо уделить особое внимание без подчеркивания их «неопытности» и сформировать гармоничный образ интернета без излишних запугиваний, с акцентами на возможностях и необходимости разумного поведения.

Технологическая основа занятий по формированию навыков безопасного поведения в сети Интернет на уровне начального общего образования.

Основные цели и задачи.

Цель: формирование основ цифровой компетентности обучающихся.

Основные задачи:

1. Формирование первоначальных представлений обучающихся о сетевом пространстве, его возможностях и рисках.

2. Формирование первоначальных навыков конструктивного использования ресурсов сети Интернет для решения образовательных, познавательных и личных задач.

3. Развитие основ критического мышления: умение критически относиться к информации, использовать несколько источников информации, с осторожностью относиться к предложениям, поступающим из незнакомых источников.

4. Освоение правил безопасного поведения в сети Интернет.

5. Формирование основ ответственного сетевого поведения; понимания необходимости обращаться за помощью в сложных случаях.

Прогнозируемые результаты в соответствии с ФГОС НОО.

При планировании результатов занятий по формированию цифровой компетентности младших школьников следует ориентироваться на требования к результатам обучающихся, освоивших основную образовательную программу начального общего образования, зафиксированных в ФГОС НОО:

Личностные результаты: развитие мотивов учебной деятельности и формирование личностного смысла учения; развитие самостоятельности и личной ответственности за свои поступки, в том числе в информационной деятельности; развитие этических чувств,

доброжелательности и эмоционально-нравственной отзывчивости; развитие навыков сотрудничества со взрослыми и сверстниками в разных социальных ситуациях, умения не создавать конфликтов и находить выходы из спорных ситуаций; формирование установки на безопасный образ жизни, наличие мотивации к работе на результат, бережному отношению к материальным и духовным ценностям.

Метапредметные результаты: овладение способностью принимать и сохранять цели и задачи учебной деятельности, поиска средств ее осуществления; освоение способов решения проблем поискового характера; определять наиболее эффективные способы достижения результата; использование знаково-символических средств представления информации для создания моделей изучаемых объектов и процессов, схем решения учебных и практических задач; активное использование средств информационных и коммуникационных технологий для решения коммуникативных и познавательных задач; использование различных способов поиска (в справочных источниках и открытом учебном информационном пространстве сети Интернет), сбора, обработки, анализа, организации, передачи и интерпретации информации в соответствии с коммуникативными и познавательными задачами и технологиями учебного предмета, в том числе умение вводить текст с помощью клавиатуры, фиксировать (записывать) в цифровой форме измеряемые величины и анализировать изображения, звуки, готовить свое выступление и выступать с аудио-, видео- и графическим сопровождением; соблюдать нормы информационной избирательности, этики и этикета; определение общей цели и путей ее достижения; овладение начальными сведениями о сущности и особенностях объектов, процессов и явлений действительности (в том числе технических); умение работать в материальной и информационной среде начального общего образования в соответствии с содержанием конкретного учебного предмета.

Предметные результаты:

Математика и информатика: овладение основами логического и алгоритмического мышления, наглядного представления данных и процессов; приобретение первоначальных представлений о компьютерной грамотности.

Обществознание и естествознание (Окружающий мир): освоение доступных способов изучения природы и общества (в том числе получение информации в открытом информационном пространстве); развитие навыков устанавливать и выявлять причинно-следственные связи.

Технология: получение первоначальных представлений о мире профессий и важности правильного выбора профессии; усвоение правил техники безопасности; приобретение первоначальных знаний о правилах создания предметной и

информационной среды и умений применять их для выполнения учебно-познавательных и проектных художественно-конструкторских задач.

Пример занятия по формированию навыков безопасного поведения в сети Интернет: сценарный план.

Тема: Безопасный интернет[19].

Цель: познакомить обучающихся начальной школы с опасностями, которые подстерегают в сети Интернет, систематизировать и обобщить сведения о безопасной работе в сети.

Задачи:

– информирование обучающихся о видах информации, способной причинить вред здоровью и развитию младших школьников, а также о негативных последствиях распространения такой информации;

– формирование у детей навыков ответственного и безопасного использования интернета на основании имеющегося у них опыта.

Ход занятия.

① Знакомство с темой занятия. Мотивация образовательной деятельности обучающихся.

В качестве видео-заставки детям можно предложить просмотр короткого видеоматериала, посвященного теме безопасного интернета.

Учитель предлагает отгадать загадку:

Сетевая паутина

оплела весь белый свет,

не пройти детишкам мимо.

Что же это? (Интернет)

Просмотр социального ролика «Безопасный интернет – детям» (ООО Видеостудия Mozga).

② Актуализация знаний.

Учитель: Мы живем в обществе, и очень многое в нашем поведении обусловлено правилами. Есть правила поведения на улице и в школе, транспорте, правила этикета. Надо ли их выполнять? Что происходит, если нарушаются правила? Приведите примеры. (Дети отвечают и приводят примеры).

[19] По материалам сайта https://infourok.ru/.

Учитель: Какие вы знаете Правила безопасности, и что будет, если их не соблюдать? (Дети отвечают: правила пожарной безопасности, поведения на дорогах, на воде и др.).

Сделаем вывод: чтобы избежать опасных ситуаций, следует слушать советы взрослых и действовать по правилам безопасности.

③ Основная часть.

Учитель: А какие же правила безопасности надо соблюдать при работе в сети Интернет? Интернет — интересный и многогранный мир, который позволяет узнавать много нового, общаться с людьми на разных концах света, играть в игры и делиться с другими своими фотографиями. Как вы думаете, какие опасности могут поджидать нас в Интернет? (Дети отвечают).

Учитель: Давайте выделим основные правила, которые нам надо соблюдать при работе в сети Интернет.

«Мы хотим, чтоб Интернет
Был вам другом много лет!
Будешь знать СЕМЬ правил этих –
Смело плавай в Интернете».

Правило 1. Никогда не публикуйте в сети и не сообщайте свое настоящее имя, адрес, школу, класс, номер телефона. Если вы разместите слишком много информации о себе, она может попасть в руки таких незнакомцев, которые используют эту информацию во вред вам.

Первый ученик: «Если кто-то незнакомый
Вас попросит рассказать
Информацию о школе,
О друзьях и телефоне,
Иль к страничке доступ дать –
Мы на это «нет» ответим,
Будем все держать в секрете!»

Правило 2. Никогда не соглашайтесь на личную встречу с людьми, с которыми вы познакомились в Интернет; под маской виртуального друга может скрываться злой человек. О подобных предложениях немедленно расскажите родителям.

Второй ученик: «Злые люди в Интернете
Расставляют свои сети.
С незнакомыми людьми
Ты на встречу не иди!»

Правило 3. Не сообщайте никому свои пароли, не посылайте СМС в ответ на письма от неизвестных людей. Будьте осторожны с вложениями и ссылками в сообщениях электронной почты.

Третий ученик: «Иногда тебе в сети
Вдруг встречаются вруны.
Обещают все на свете
Подарить бесплатно детям:
Телефон, щенка, айпод
и поездку на курорт.
Их условия не сложны:
СМС отправить можно
С телефона папы, мамы –
И уже ты на Багамах.
Ты мошенникам не верь,
Информацию проверь».

Правило 4. Всегда сообщайте взрослым обо всех случаях в интернет, которые вызвали у вас смущение или тревогу.

Четвертый ученик: «Если что-то непонятно,
Страшно или неприятно,
Быстро к взрослым поспеши,
Расскажи и покажи.
Есть проблемы в Интернете?
Вместе взрослые и дети
Могут все решить всегда
Без особого труда».

Правило 5. Для того, чтобы избежать встречи с неприятной информацией в Интернет, установите на свой браузер фильтр или попросите сделать это взрослых – тогда ты сможешь смело путешествовать по интересным тебе страницам.

Пятый ученик: «Как и всюду на планете,
Есть опасность в Интернете.
Мы опасность исключаем,
Если фильтры подключаем».

Правило 6. Не скачивайте и не открывайте незнакомые файлы, не спросив разрешения родителей или учителей. Если же решили что-то скачать, проверьте файл с помощью антиирусной программы перед тем, как открыть его.

Шестой ученик: «Не хочу попасть в беду –

Антивирус заведу!

Всем, кто ходит в Интернет,

Пригодится наш совет».

Правило 7. При общении в Интернете вы должны быть дружелюбными с другими пользователями. Ни в коем случае не надо писать и говорить оскорбительные слова, нельзя опубликовывать в сети чужие фотографии и сведения без разрешения хозяина.

Седьмой ученик: «С грубиянами в сети

Разговор не заводи.

Ну и сам не оплошай –

Никого не обижай».

Учитель: Ребята, если Вы будете соблюдать эти правила, то Интернет станет для Вас верным помощником, ведь в Интернет можно искать информацию, читать книги, посещать виртуальные музеи, играть, общаться с друзьями и конечно, учиться.

④ Закрепление.

Учитель: А теперь проверим, насколько хорошо Вы усвоили правила безопасного поведения в Интернете. Попробуйте сформулировать основные правила, используя хорошо известные сказки. Учитель демонстрирует картинки из сказок, учащиеся формулируют правила.

– «Красная шапочка» (Будь осторожен в общении с незнакомцами).

– «Волк и семеро козлят» (Под маской виртуального друга может скрываться злой человек).

– «Золотой ключик, или Приключения Буратино» (Опасайся мошенников. Не сообщай никому свои пароли, не посылай смс в ответ на письма от неизвестных людей).

– «Сестрица Алёнушка и братец Иванушка» (При встрече с неприятной (грязной) информацией в сети, выйди из интернета. Всегда советуйся со старшими относительно поведения в сети).

– «Морозко» (Будь вежливым при общении в сети, не груби, тогда и к тебе будут относиться так же).

⑤ Рефлексия (подведение итогов занятия).

– О чем мы сегодня говорили на занятии?

– Какие основные правила безопасности в сети Интернет мы сегодня обсуждали?

– Как вы можете использовать полученную на занятии информацию в повседневной жизни?

Памятка школьнику: основные правила безопасного поведения в сети Интернет обучающегося начальной школы.

1. Всегда спрашивайте родителей или учителей о незнакомых вещах в интернете. Они расскажут, что безопасно делать, а что нет. Прежде чем начать дружить с кем-то в интернете, спросите у родителей как безопасно общаться.

2. Никогда не рассказывайте о себе незнакомым людям. Где вы живете, в какой школе учитесь, номер телефона – это должны знать только ваши друзья и семья.

3. Не отправляйте фотографии людям, которых вы не знаете. Незнакомые люди не должны видеть фотографии Ваши, Ваших друзей или семьи.

4. Не встречайтесь без родителей с людьми из интернета вживую. В интернете многие люди рассказывают о себе неправду.

5. Если вас кто-то расстроил или обидел, обязательно расскажите родителям.

ОСНОВНОЕ ОБЩЕЕ ОБРАЗОВАНИЕ

Возрастные особенности обучающихся основной школы в контексте развития навыков безопасного поведения в сети Интернет.

Подростковый возраст – сложный период, в который происходит становление личности. Вместе с тем это очень ответственный этап взросления, поскольку складываются основы нравственности, формируются социальные установки, отношения к себе, к людям, к обществу. В данном возрасте стабилизируются черты характера и основные формы межличностного поведения. Главные мотивационные линии этого возрастного периода, связанные с активным стремлением к личностному самосовершенствованию – это самопознание, самовыражение и самоутверждение.

В начале подросткового возраста у ребенка появляется и усиливается стремление быть похожим на старших, детей и взрослых. Сами взрослые начинают относиться к подросткам уже не как к детям, а более серьезно и требовательно. Итогом этих процессов становится укрепляющееся внутреннее стремление подростка поскорее стать взрослым, которое создает совершенно новую внешнюю и внутреннюю ситуацию личностного психологического развития. Роль подражания в развитии личности подростка изменяется, оно перестает быть стихийным, становится управляемым, начинает обслуживать многочисленные потребности интеллектуального и личностного самосовершенствования ребенка. Поэтому важно, чтобы в ближайшем окружении подростка были примеры разумного и ответственного поведения в сетевом пространстве.

В подростковом и юношеском возрасте активно идет процесс познавательного развития, активно развивается логическая память. Процесс запоминания сводится к мышлению, к установлению логических отношений внутри запоминаемого материала. Подростки начинают мыслить логически, заниматься теоретическими рассуждениями и самоанализом. Таким образом, формирование навыков безопасного сетевого поведения в подростковом возрасте должно строиться на обсуждении, быть теоретически подкреплено, все значимые выводы должны быть логически обоснованы.

Еще одной чертой, которая впервые полностью раскрывается именно в подростковом возрасте, является склонность к экспериментированию, подростки обнаруживают широкие познавательные интересы, связанные со стремлением все самостоятельно перепроверить, лично удостовериться в истинности. В этом таится опасность – подросток, в силу недостаточного жизненного опыта, наиболее восприимчив к интернет-рискам, уязвим.

В общении развиваются коммуникативные способности, при этом основная часть общения приходится на ближний круг: друзья, одноклассники, знакомые взрослые (учителя, тренеры и т.д.), родители. Умение вступать в контакт с незнакомыми людьми только начинает развиваться и формируется к концу основной школы. На этом этапе резко возрастает коммуникативная активность, что влечет за собой нарастание рисков в сфере интернет-коммуникаций.

Детей этого возраста отличает повышенный интерес к различным видам деятельности, стремление что-то делать своими руками, повышенная любознательность и первые мечты о будущей профессии. Первичные профессиональные интересы зарождаются в школе, дома, во внешкольных делах. И здесь формирование цифровой грамотности может лечь в основу будущей профессиональной деятельности.

Дети 10-12 лет уже, как правило, знают, как использовать интернет в различных целях. Родители могут поддержать ребенка, выяснив, какие сайты могут помочь с домашним заданием, содержат информацию о хобби или других увлечениях ребенка. Интернет может также использоваться для планирования вопросов, касающихся всей семьи. Это дает возможность родителям и детям обсудить надежность разных сайтов, а также источники поиска полезной и качественной информации. Ребенку необходим родительский присмотр и контроль, а также знание правил безопасной и продуктивной работы в сети. Родителям и детям необходимо прийти к соглашению относительно разрешенных и запрещенных действий в Интернете, а также его использования. В соглашении должны быть учтены все потребности и мнения. Договоритесь, какую личную информацию можно разглашать и в каких случаях, а также поговорите о рисках,

связанных с разглашением информации. Если ребенок уже заинтересовался общением в чатах, вам следует обсудить с детьми их безопасность и контролировать их опыт в интерактивных обсуждениях. Технические средства, обеспечивающие безопасность информации также необходимо обновлять.

В возрасте 13–15 лет интернет становится частью социальной жизни: в сети подростки знакомятся и проводят время, ищут информацию, связанную с учебой или увлечениями. При высоком уровне грамотности использование интернета открывает множество возможностей. Подростки, как правило, выстраивают личностные границы, оберегают свое личное пространство, что увеличивает дистанцию между ребенком и родителям. Это усложняет возможности родительской медиации активности подростков в интернете. Дети 13–15 лет могут сохранять свои действия в тайне, особенно если родители раньше не интересовались деятельностью ребенка в Интернете. Тем не менее контроль необходим, в этом возрасте дети склонны к риску и выходу за пределы дозволенного. Технические ограничения и запреты могут оказаться неэффективным способом повышения уровня сетевой безопасности. Важным моментом для семьи становится участие в открытых дискуссиях, а для родителей – заинтересованность жизнью ребенка в интернете.

Технологическая основа занятий по формированию навыков безопасного поведения в сети Интернет на уровне основного общего образования.

Основные цели и задачи.

Цель: формирование и развитие цифровой компетентности обучающихся.

Основные задачи:

1. Развитие представлений обучающихся о сетевом пространстве, его возможностях и рисках, деятельности в сети.

2. Формирование и развитие навыков конструктивного использования ресурсов сети Интернет для решения образовательных, познавательных и личных задач.

3. Формирование навыков конструктивного общения в сети Интернет.

4. Развитие критического мышления.

5. Формирование навыков безопасного поведения в сети Интернет.

6. Формирование ответственного сетевого поведения.

7. Формирование представлений о правонарушениях и преступлениях в сети.

8. Профилактика зависимого поведения (интернет-зависимости).

Прогнозируемые результаты в соответствии с ФГОС ООО.

При планировании результатов занятий по формированию цифровой компетентности детей среднего школьного возраста следует ориентироваться на требования к результатам обучающихся, освоивших основную образовательную программу основного общего образования, зафиксированных в ФГОС ООО:

Личностные результаты: формирование готовности и способности обучающихся к саморазвитию и самообразованию; освоение социальных норм, правил поведения, ролей и форм социальной жизни в группах и сообществах; формирование осознанного и ответственного отношения к собственным поступкам; формирование коммуникативной компетентности в общении и сотрудничестве со сверстниками, детьми старшего и младшего возраста, взрослыми в процессе разных видов деятельности; усвоение правил индивидуального и коллективного безопасного поведения.

Метапредметные результаты: умение самостоятельно ставить цели и планировать пути их достижения, в том числе альтернативные, осознанно выбирать наиболее эффективные способы решения учебных и познавательных задач; умение соотносить свои действия с планируемыми результатами, осуществлять контроль своей деятельности в процессе достижения результата, корректировать свои действия в соответствии с изменяющейся ситуацией; владение основами самоконтроля, самооценки, принятия решений и осуществления осознанного выбора в учебной и познавательной деятельности; формирование и развитие компетентности в области использования информационно-коммуникационных технологий; развитие мотивации к овладению культурой активного пользования разными поисковыми системами;

Предметные результаты:

Обществознание: формирование основ правосознания для соотнесения собственного поведения и поступков других людей с нравственными ценностями и нормами поведения, установленными законодательством Российской Федерации; освоение приемов работы с социально значимой информацией, ее осмысление.

Математика. Алгебра. Геометрия. Информатика: овладение навыками инструментальных вычислений; развитие умений применять изученные понятия, результаты, методы для решения задач практического характера и задач из смежных дисциплин с использованием при необходимости справочных материалов, компьютера; формирование информационной и алгоритмической культуры; формирование представления о компьютере как универсальном устройстве обработки информации; развитие основных навыков и умений использования компьютерных устройств; формирование представления об основных изучаемых понятиях: информация, алгоритм,

модель – и их свойствах; знакомство с одним из языков программирования; формирование навыков и умений безопасного и целесообразного поведения при работе с компьютерными программами и в Интернете, умения соблюдать нормы информационной этики и права.

Технология: осознание роли техники и технологий для прогрессивного развития общества; формирование целостного представления о техносфере, сущности технологической культуры; развитие умений применять технологии представления, преобразования и использования информации, оценивать возможности и области применения средств и инструментов ИКТ в современном производстве или сфере обслуживания; формирование представлений о мире профессий, связанных с изучаемыми технологиями, их востребованности на рынке труда.

Основы безопасности жизнедеятельности: формирование современной культуры безопасности жизнедеятельности; формирование убеждения в необходимости безопасного жизни; знание основных опасных ситуаций (в том числе техногенного и социального характера); знание и умение применять меры безопасности и правила поведения в условиях опасных ситуаций; умение предвидеть возникновение опасных ситуаций; умение принимать обоснованные решения в конкретной опасной ситуации с учетом реально складывающейся обстановки и индивидуальных возможностей.

Пример занятия по формированию навыков безопасного поведения в сети Интернет: сценарный план.

Тема: Кибербуллинг и борьба с ним.

Цели и задачи:

– знакомство с понятием буллинга и кибербуллинга;

– обсуждение последствий кибербуллинга.

Ход занятия.

① Знакомство с темой занятия. Мотивация образовательной деятельности обучающихся.

Учитель знакомит детей с понятием «кибербуллинг».

② Актуализация знаний.

Просмотр и обсуждение видеоматериала «Что такое кибербуллинг и как от него защититься» (Региональная общественная организация «Центр Интернет-технологий» (РОЦИТ), 2018г.) (Режим доступа: https://www.youtube.com/watch?v=bGmnK_ruQ-M).

③ Основная часть.

Учитель: сталкиваясь с проблемами в Сети, дети и подростки часто не знают, как поступить в неприятной или опасной ситуации и куда можно обратиться за помощью. Для оказания психологической помощи и улучшения осведомленности детей и взрослых о способах решения сложных ситуаций, возникающих при пользовании интернетом, в декабре 2009 года начала свою работу линия помощи «Дети Онлайн». Линия помощи «Дети Онлайн» – служба телефонного и онлайн-консультирования по проблемам безопасного использования сети Интернет и мобильной связи для детей, подростков, родителей и работников образовательных организаций.

Учитель просит участников представить, что они работают на этой линии. Каждый день им звонят и пишут их сверстники с просьбой помочь решить проблемы, возникшие в интернете.

Работа в группах.

Каждая группа получает карточку с запросом, который поступил на линию помощи «Дети онлайн» по электронной почте. Все истории на карточках – реальные запросы, имена обратившихся изменены.

Участникам групп в течение 10 минут необходимо ознакомиться с письмом, обсудить его в группе, подготовить ответы на следующие вопросы:

– Как чувствует себя автор письма?

– Что ему следует делать в этой ситуации? (Составьте пошаговые рекомендации)

– Кто ему может помочь?

– Стоит ли ему обратиться за помощью?

Итоги групповой работы озвучиваются. Предложенные рекомендации фиксируются на доске, другие группы могут их дополнять.

Подводя итог работы, учитель резюмирует и дополняет рекомендации. Получается стратегия (или несколько вариантов стратегий) поведения в ситуации кибербуллинга.

④ Закрепление.

Учитель рассказывает детям об организациях, созданных добровольцами, которые оказывают поддержку подросткам, подвергающимся кибербуллингу. Они помогают не только советами, они общаются и с ними в интернете, встречаются в реальной жизни, чтобы вместе решить проблему.

Работа в группах.

Учитель предлагает представить, что в их школе есть группа помощи школьникам, подвергающихся буллингу и кибербуллингу. Она называется «Старший брат», в нее входят ученики из разных классов. Каждая группа должна придумать свое мероприятие, целью которого будет привлечение внимания школьников к проблеме кибербуллинга,

повышение осведомленности в сфере безопасного сетевого общения. Участникам дается 10 минут на подготовку проекта: они должны придумать название мероприятия, план проведения (сценарий) и ожидаемые результаты.

⑤ Рефлексия (подведение итогов занятия).

Проекты обсуждаются в классе. Затем проходит голосование, лучшая идея может быть реализована в школе.

В помощь учителю: материалы к занятию.

Материалы для групповой работы.

Письмо 1.

Здравствуйте, меня зовут Мария, мне 14 лет. Недавно я была в гостях у двоюродных братьев и с их компьютера заходила на свою страничку в социальной сети, но не вышла перед тем, как уйти из гостей. Братья разослали всем моим друзьям неприличные картинки, а на моей стене написали оскорбительные сообщения про всех моих знакомых. Что же мне делать? Что подумают мои друзья? Удалять страницу очень не хочется. Хочу отомстить своим братьям, хотя и понимаю, что это неправильно.

Письмо 2.

Петя, 13 лет. Доброго времени суток! Мой одноклассник создал группу в популярной социальной сети «Истории Пети Петухова». Страничка повергла меня в шок! Он и его друзья пишут насмешливые и издевательские истории, где выставляют меня дураком! Еще они выложили мои фотографии, которые взяли с моей странички и сделали гадкие подписи! Пишут, что я тупой, а все мои пятерки потому, что моя мама дружит с директором! Но это не так, мне просто нравится учиться. Техпомощь социальной сети не откликается на просьбы удалить эту страницу! А они не перестают, каждый день выкладывают все новые гадкие истории и приглашают в группу моих друзей из социальной сети. Одна девочка пробовала меня защищать, писала на стене, чтобы они закрыли группу, но они не послушались, боюсь, как бы они за нее не взялись. Мне очень плохо от их гадких комментариев, все чаще по утрам я не хочу идти в школу, чтобы не видеть лица обидчиков. Умоляю вас, пожалуйста, помогите.

Письмо 3.

Катя, 14 лет. Здравствуйте! Общалась вчера в соцсети – и вдруг получила сообщение от какой-то девушки. Я ее не знаю. Возраст у нее не написан, но, судя по фотографиям, ей лет 20-25. У меня достаточное количество друзей, которые добавились сами. Я хотела удалить их, но всех не смогла, и в подписках осталось 600 с лишним человек. Я не занималась никаким пиаром и абсолютно никого не трогала, но меня начали

унижать. Не хочу перечислять все, что говорила эта девушка. Затем она на моей стене стала помещать неприятную и ложную информацию. Мало того, она попросила своих друзей сделать то же самое. Теперь я боюсь сидеть в соцсети, потому что думаю, это будет продолжаться. Сегодня пока что тихо, но я не знаю, что будет дальше. Спасибо заранее за помощь!

Письмо 4.

Оля, 15 лет. Моя лучшая подруга сейчас переживает из-за одной проблемы. Ей 17 лет, в 15 она создала страничку под видом мальчика, с чужим именем и с чужими фотографиями, и общалась с девочкой, девочка влюбилась. Моя подруга всячески пыталась отделаться от нее, а та переживала очень, нервничала и плакала. Моя подруга сейчас боится, что ей что-то будет за то, что в Интернете два года она обманывала девочку, а та влюбилась. Сейчас уже месяц она с ней не общается. Что будет моей подруге, если та девочка захочет обратиться в суд, и вообще возможно ли такое? Что делать? Спасибо!

Письмо 5.

Роман. Я учусь в седьмом классе. И надо мной издеваются ребята из старших классов. Они сняли видео, как они бьют меня и толкают в туалете, плюют и пинают ногами. Теперь грозятся выложить его в соцсети, если я не буду им отдавать все карманные деньги. А еще совсем недавно на мою страницу в социальной сети стали приходить оскорбительные, гадкие сообщения. Они оскорбляют не только меня, но и мою маму, и тетю! Обещают создать группу «АнтиИвановы» и добавить всех моих друзей туда. Сообщения приходят от незнакомцев, страницы выдуманные, но я почти уверен, что это те, кто бьет меня. Я боюсь выходить на улицу, боюсь, что они забьют меня до смерти. Что делать? Помогите мне.

Рекомендации по борьбе с кибербуллингом.

1. При общении в интернете оставайтесь дружелюбными с другими пользователями. Не стоит писать резкие и оскорбительные слова – читать грубости так же неприятно, как и слышать. Жестокое обращение и грубые слова могут привести к насилию, самоубийствам, депрессии и дискриминации внутри школьной среды.

2. Научитесь правильно реагировать на обидные слова или действия других пользователей.

3. Не стоит общаться с агрессором и тем более пытаться ответить ему тем же. Возможно, стоит вообще покинуть данный ресурс и удалить оттуда свою личную информацию, если не получается решить проблему мирным путем. Лучший способ

испортить хулигану его выходку – отвечать ему полным игнорированием.

4. Личная информация, которую пользователи выкладывают в интернете, а также фотографии могут быть использованы агрессорами против них.

Доверие и помощь.

5. Если человек столкнулся с травлей, оскорблениями в интернете, помогите ему найти выход из ситуации – практически на всех форумах и сайтах есть возможность заблокировать обидчика, написать жалобу модератору или администрации сайта, потребовать удаление странички.

6. Убедитесь, что оскорбления (буллинг) из сети не перешли в реальную жизнь. Если поступающие угрозы касаются жизни или здоровья жертвы, а также членов его семьи, то они имеют право на защиту со стороны правоохранительных органов, а действия обидчиков могут попадать под статьи уголовного и административного кодексов о правонарушениях.

7. Если у вас есть информация, что кто-то из друзей или знакомых вашего друга или одноклассника подвергается буллингу или кибербуллингу, то сообщите об этом классному руководителю или школьному психологу.

Памятка школьнику: основные правила безопасного поведения в сети Интернет обучающегося основной школы.

1. При регистрации на сайтах, старайтесь не указывать личную информацию, т.к. она может быть доступна незнакомым людям. Так же не рекомендуется размещать свою фотографию, давая, тем самым, представление о том, как вы выглядите, посторонним людям.

2. Используйте веб-камеру только при общении с друзьями. Проследите, чтобы посторонние люди не имели возможности видеть ваш разговор, т.к. он может быть записан.

3. Нежелательные письма от незнакомых людей называются «спам». Если вы получили такое письмо, не отвечайте на него. В случае, если Вы ответите на подобное письмо, отправитель будет знать, что вы пользуетесь своим электронным почтовым ящиком и будет продолжать посылать вам спам.

4. Если вам пришло сообщение с незнакомого адреса, его лучше не открывать. Подобные письма могут содержать вирусы или иные вредоносные программы и файлы.

5. Если вам приходят письма с неприятным и оскорбляющим вас содержанием, если кто-то ведет себя в вашем отношении неподобающим образом, сообщите об этом взрослым.

6. Если вас кто-то расстроил или обидел, расскажите об этом взрослым.

СРЕДНЕЕ ОБЩЕЕ ОБРАЗОВАНИЕ

Возрастные особенности обучающихся старшей школы в контексте развития навыков безопасного поведения в сети Интернет.

Ранняя юность – время перехода к настоящей взрослости, первые признаки которой появляются в подростковом возрасте. На период ранней юности, традиционно связываемый с обучением в старших классах школы, приходится становление нравственного самосознания. Если для детей младшего школьного возраста источником постановки и решения нравственных проблем являются значимые взрослые – родители и учителя, подростки, кроме того, ищут их решения в кругу сверстников, то юноши и девушки в поисках правильного ответа на те же самые вопросы обращаются к источникам, которыми обычно пользуются взрослые люди: реальные человеческие отношения, литература, произведения искусства, интернет и т. п.

Для юности характерно повышенное внимание к внутреннему миру человека, это, как правило, мысли о людях, о мире, о философских, бытовых и других проблемах. Все они личностно затрагивают и волнуют старших школьников. В юности нередко встречается обостренное чувство одиночества. Все это является фактором повышенного риска для вовлечение молодых людей в деструктивные интернет-сообщества, например, суицидальной, религиозной, экстремистской направленности. К счастью, чувство одиночества в юности не является стабильным, при установлении хороших личных контактов с окружающими людьми оно быстро исчезает.

В ранней юности по сравнению с отрочеством значительно снижается острота межличностных конфликтов и в гораздо меньшей степени проявляется негативизм во взаимоотношениях с окружающими людьми, появляется больше доверия к чужому опыту. Таким образом, юноши меньше подростков подвержены интернет-рискам в сфере коммуникаций, и чаще демонстрируют готовность к присвоению чужого позитивного опыта сетевого поведения.

Для современных молодых людей характерен открытый, непредвзятый и смелый взгляд на мир, включая постановку и решение многих проблем морально-этического характера, самостоятельность – хотя и не всегда правильность – суждений. Самостоятельность мышления проявляется независимо от выбора способа поведения, юноши принимают лишь то, что лично им кажется разумным, целесообразным и полезным. Соответственно формирование безопасного поведения в этом возрасте должно

строиться на обращении к опыту молодых людей, постановке исследовательских задач, инициировании дискуссий, в результате чего они смогут придти к самостоятельным выводам в рамках обсуждаемой проблематики.

Ранняя юность – начало практической реализации жизненных планов, которые складываются к концу подросткового возраста. Близость к завершению школы требует профессионального и личностного самоопределения. Увлеченность современными технологиями, развитая цифровая компетентность могут стать основание для выбора будущей профессии.

К окончанию школы большая часть юношей и девушек представляет собой людей практически нравственно сформированных, обладающих достаточно устойчивой моралью, определенными способностями, мотивами и чертами характера. Поэтому так важно именно в школьные годы сформировать цифровую компетентность ребенка, включая такой важный аспект как навыки безопасного поведения в интернет-среде.

Технологическая основа занятий по формированию навыков безопасного поведения в сети Интернет на уровне среднего общего образования.

Основные цели и задачи.

Цель: развитие цифровой компетентности обучающихся.

Основные задачи:

1. Развитие представлений обучающихся о сетевом пространстве, его возможностях и рисках, деятельности в сети.

2. Развитие навыков конструктивного использования ресурсов сети Интернет для решения образовательных, познавательных и личных задач.

3. Развитие навыков конструктивного общения в сети Интернет.

4. Развитие критического мышления.

5. Развитие навыков безопасного поведения в сети Интернет.

6. Формирование ответственного сетевого поведения.

7. Развитие представлений о правонарушениях и преступлениях в сети, о юридической ответственности за собственные поступки в сети.

8. Профилактика зависимого поведения (интернет-зависимости).

Прогнозируемые результаты в соответствии с ФГОС СОО.

При планировании результатов занятий по формированию цифровой компетентности старших школьников следует ориентироваться на требования к

результатам обучающихся, освоивших основную образовательную программу среднего общего образования, зафиксированных в ФГОС СОО:

Личностные результаты: готовность и способность к самостоятельной и ответственной деятельности; способность противостоять идеологии экстремизма, национализма, ксенофобии, дискриминации по социальным, религиозным, расовым, национальным признакам и другим негативным социальным явлениям; готовность и способность к образованию, в том числе самообразованию, на протяжении всей жизни; принятие и реализация ценностей безопасного образа жизни; бережное, ответственное и компетентное отношение к психологическому здоровью, как собственному, так и других людей; осознанный выбор будущей профессии и возможностей реализации собственных жизненных планов.

Метапредметные результаты: использовать все возможные ресурсы для достижения поставленных целей и реализации планов деятельности; выбирать успешные стратегии в различных ситуациях; умение продуктивно общаться и взаимодействовать в процессе совместной деятельности; владение навыками познавательной, учебно-исследовательской и проектной деятельности, навыками разрешения проблем; способность и готовность к самостоятельному поиску методов решения практических задач, применению различных методов познания; готовность и способность к самостоятельной информационно-познавательной деятельности, умение ориентироваться в различных источниках информации, критически оценивать и интерпретировать информацию, получаемую из различных источников; умение использовать средства информационных и коммуникационных технологий в решении когнитивных, коммуникативных и организационных задач с соблюдением требований эргономики, техники безопасности, гигиены, ресурсосбережения, правовых и этических норм, норм информационной безопасности.

Предметные результаты:

Обществознание (базовый уровень): сформированность представлений об основных тенденциях и возможных перспективах развития мирового сообщества в глобальном мире; владение умением прогнозировать последствия принимаемых решений; сформированность навыков оценивания социальной информации, умений поиска информации в источниках различного типа.

Экономика (базовый уровень): владение навыками поиска актуальной экономической информации в различных источниках, включая Интернет; умение различать факты, аргументы и оценочные суждения.

Право (базовый уровень): владение знаниями о правонарушениях и юридической ответственности; сформированность навыков самостоятельного поиска правовой информации, умений использовать результаты в конкретных жизненных ситуациях.

Математика (включая алгебру и начала математического анализа, геометрию) (базовый уровень): владение навыками использования готовых компьютерных программ при решении задач.

Информатика (базовый уровень): сформированность представлений о роли информации и связанных с ней процессов в окружающем мире; использование готовых прикладных компьютерных программ по выбранной специализации; сформированность представлений о способах хранения и простейшей обработке данных; понятия о базах данных и средствах доступа к ним, умений работать с ними; владение компьютерными средствами представления и анализа данных; сформированность базовых навыков и умений по соблюдению требований техники безопасности, гигиены и ресурсосбережения при работе со средствами информатизации; понимания основ правовых аспектов использования компьютерных программ и работы в Интернете.

Основы безопасности жизнедеятельности (базовый уровень): сформированность представлений о культуре безопасности жизнедеятельности; знание основ российского законодательства, направленных на защиту населения от внешних и внутренних угроз; сформированность представлений о необходимости отрицания экстремизма, терроризма, других действий противоправного характера, а также асоциального поведения; умение предвидеть возникновение опасных ситуаций по характерным для них признакам, а также использовать различные информационные источники; умение применять полученные знания в области безопасности на практике, проектировать модели личного безопасного поведения в повседневной жизни.

Пример занятия по формированию навыков безопасного поведения в сети Интернет: сценарный план.

Тема: Интернет-зависимость.

Цель: актуализировать представление обучающихся об интернет-зависимости, выработать стратегии профилактики этого явления.

Задачи:

– информирование обучающихся об интернет-зависимости, ее видах, опасности зависимого поведения, возможностях профилактики этого явления;

– развитие навыков ответственного и безопасного использования интернета.

Ход занятия.

① Знакомство с темой занятия. Мотивация образовательной деятельности обучающихся.

В качестве введения в тему занятия можно предложить просмотр короткого видеоматериала, посвященного теме интернет-зависимости.

② Актуализация знаний.

Учитель организует дискуссию о таком явлении, как интернет-зависимость, с опорой на вопросы:

– Что такое интернет-зависимость? Что включает это понятие?

– Существует ли такая проблема в современном мире?

– Сталкивались ли Вы с этой проблемой?

③ Основная часть.

Рассказ учителя.

Проблема интернет-зависимости появилась с возрастанием популярности сети Интернет. Некоторые люди настолько увлеклись виртуальным пространством, что начали предпочитать интернет реальности, проводя за компьютером до 18 часов в сутки. Отказ от интернета вызывает у таких людей тревогу и эмоциональное возбуждение. Психиатры усматривают схожесть такой зависимости с чрезмерным увлечением азартными играми. Официально медицина пока не признала интернет-зависимость психическим расстройством, некоторые эксперты в области психиатрии вообще сомневаются в существовании интернет-зависимости или отрицают вред от этого явления.

По данным различных исследований, интернет-зависимыми сегодня являются около 10% пользователей во всём мире. Российские психиатры считают, что сейчас в нашей стране таковых 4-6%. Несмотря на отсутствие официального признания проблемы, интернет-зависимость уже принимается в расчёт во многих странах мира. Например, в Финляндии молодым людям с интернет-зависимостью предоставляют отсрочку от армии.

Основные типы интернет-зависимости таковы:

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

2. Пристрастие к виртуальному общению и виртуальным знакомствам – большие объёмы 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.

Работа в группах.

Обучающие объединяются в группы и обсуждают следующие вопросы:

– Какие «плюсы» есть в нашей жизни благодаря интернету?

– Какие «минусы» привнес (реальные и потенциальные) в нашу жизнь интернет?

– Обеднела бы наша жизнь, если бы не было интернета? Насколько сильно? В каких сферах это проявилось бы особенно сильно?

– Какие «плюсы», возможно, появились бы в нашей жизни, если бы интернет «пропал» на какое-то время?

Результаты групповой работы выносятся на общее обсуждение. Формулируются и фиксируются основные выводы.

④ Закрепление.

Работа в группах.

Учитель предлагает детям представить, что они выросли и стали родителями. Их ребенок стал чрезмерно много времени проводить в сети. Что можно предпринять в такой ситуации? Сформулируйте правила и рекомендации.

⑤ Рефлексия (подведение итогов занятия).

Результаты групповой работы выносятся на общее обсуждение. Формулируются и фиксируются основные выводы.

Памятка школьнику: основные правила безопасного поведения в сети Интернет обучающегося старшей школы.

1. Нежелательно размещать персональную информацию в интернете. Персональная информация – это номер вашего мобильного телефона, адрес электронной почты, домашний адрес и фотографии вас, вашей семьи или друзей.

2. Помните, если вы публикуете фото или видео в интернете, каждый может посмотреть их и использовать со злым умыслом.

3. Не отвечайте на нежелательные электронные письма от незнакомых людей и с незнакомых электронных адресов.

4. Не открывайте файлы, которые прислали неизвестные вам люди. Вы не можете знать, что на самом деле содержат эти файлы – в них могут быть вирусы или фото/видео с «агрессивным» содержанием.

5. Не добавляйте незнакомых людей в свой контакт-лист в социальных сетях и интернет-месседжерах.

6. Помните, что виртуальные знакомые могут быть не теми, за кого себя выдают.

7. Если рядом с вами нет взрослых людей, не встречайтесь в реальной жизни с людьми, с которыми вы познакомились в интернете.

8. Если ваш виртуальный друг действительно тот, за кого он себя выдает, он нормально отнесется к вашей заботе о собственной безопасности.

9. Никогда не поздно рассказать взрослым, если вас кто-то обидел.

Полезные информационные ресурсы.

Важным показателем информационного общества является все возрастающая скорость технологических изменений. В информационном обществе приоритетной становится высокая степень образованности, только образованные люди способны эффективно использовать информацию как мощный ресурс. На сегодняшний день человеку недостаточно просто получить образование, требуется постоянное обновление знаний.

Современный мир предъявляет свои требования: нужно быть в курсе всего нового, непрерывно повышать свою профессиональную квалификацию, обмениваться опытом с коллегами, отслеживать, успевать прочитывать и анализировать разные источники информации. Рекомендованные информационные ресурсы могут помочь педагогам лучше ориентироваться в тематическом проблемном поле, повысить собственную цифровую компетентность, подобрать материалы для организации и проведения занятий по формированию у обучающихся навыков безопасного поведения в сети Интернет, а также для ведения просветительской деятельности с родителями обучающихся.

→ *Информационный ресурс:* Центр безопасного интернета в России.

Ссылка: http://www.saferunet.ru/

Комментарий: Центр безопасного Интернета в России является уполномоченным российским членом Европейской сети Центров безопасного Интернета (Insafe), действующей в рамках Safer Internet Programme Европейской Комиссии и объединяющей национальные Центры безопасного Интернета стран ЕС и России. Рекомендован Уполномоченным при Президенте Российской Федерации по правам ребенка, организатор сайта – Общественная палата Российской Федерации.

→ *Информационный ресурс:* Фонд содействия развитию сети Интернет «Дружественный Рунет».

Ссылка: http://www.friendlyrunet.ru/safety/

Комментарий: главной целью Фонда является содействие развитию сети Интернет как благоприятной среды, дружественной ко всем пользователям. Фонд поддерживает проекты, связанные с безопасным использованием интернета, содействует российским пользователям, общественным организациям, коммерческим компаниям и государственным ведомствам в противодействии обороту противоправного контента, а также в противодействии иным антиобщественным действиям в Сети.

Фонд «Дружественный Рунет» реализует в России комплексную стратегию в области безопасного использования интернета. Основными проектами Фонда являются: Горячая линия по приему сообщений о противоправном контенте, специализированная линия помощи для детей «Дети онлайн» и просветительские проекты.

→ *Информационный ресурс:* Региональная общественная организация «Центр Интернет-технологий».

Ссылка: https://rocit.ru/

Комментарий: РОЦИТ – это общественная организация, объединяющая активных интернет-пользователей России. Цель РОЦИТ – содействовать развитию и распространению интернет-технологий в интересах граждан России. РОЦИТ реализует образовательные проекты в области IT и цифровой грамотности, представляет актуальные исследования интернет-пользования (анализ востребованности и актуальности оказываемых интернет-услуг), защищает интересы пользователей и специалистов интернет-сферы на государственном уровне и с представителями бизнеса, развивает культуру потребления интернета среди граждан.

→ *Информационный ресурс:* Дети России Онлайн.

Ссылка: http://detionline.com/

Комментарий: Дети России Онлайн – сайт Фонда Развития Интернет. Фонд реализует проекты, посвященные вопросам социализации детей и подростков в развивающемся информационном обществе, а также проблемам их безопасности в современной инфокоммуникационной среде.

→ *Информационный ресурс:* ФГБНУ «Центр защиты прав и интересов детей» «Твой безопасный кибермаршрут».

Ссылка: https://www.fcprc.ru/projects/cyberbullying

Комментарий: система консультативной помощи подросткам и родителям в области информационной безопасности в сети Интернет.

→ *Информационный ресурс:* «Защита детей» – информационный сайт Лаборатории Касперского.

Ссылка: https://kids.kaspersky.ru/

Комментарий: на сайте представлены новости, статьи, игры и рекомендации по защите ребенка в сети Интернет.

→ *Информационный ресурс:* Лига безопасного интернета.

Ссылка: http://www.ligainternet.ru/

Комментарий: цель Лиги безопасного интернета: искоренение опасного контента путем самоорганизации профессионального сообщества, участников интернет-рынка и рядовых пользователей.

→ *Информационный ресурс:* Ассоциация электронных коммуникаций (РАЭК) «WWW.I-DETI.ORG».

Ссылка: http://i-deti.org/

Комментарий: безопасный интернет для детей: законодательство, советы, мнения, международный опыт.

→ *Информационный ресурс:* Детская страница портала «Персональные данные».

Ссылка: http://xn--80aalcbc2bocdadlpp9nfk.xn--d1acj3b/

Комментарий: различные материалы, разработанные специалистами Роскомнадзора, для педагогов и родителей, которые хотят помочь детям понять важность конфиденциальности личной жизни при использовании цифровых технологий, а также для молодых людей, которые используют среду Интернет. Материалы страницы должны помочь детям понять последствия, которые информационные технологии могут оказать на личную жизнь, и предоставить инструменты и информацию, необходимые для принятия решений в вопросах виртуальной жизни.

→ *Информационный ресурс:* Комплексный социальный проект «НеДопусти!».

Ссылка: http://nedopusti.ru/site/page/aboutproject/

Комментарий: проект ориентирован на противодействие цифровым угрозам, современному рабству и опасностям для детей. Одна из основных задач проекта – поставить возможности высоких технологий на службу делу защиты и безопасности детей, обеспечению их полноценного развития и саморазвития. Организаторами проекта являются Общественная палата РФ, РОЦИТ (Региональная Общественная Организация «Центр Интернет-технологий»), Межрегиональная правозащитная общественная организация «Сопротивление».

→ *Информационный ресурс:* Издательство «Образование и Информатика» (ИНФО).

Ссылка: http://infojournal.ru/

Комментарий: издательство выпускает два периодических издания – журналы «Информатика и образование» и «Информатика в школе», а также научно-методическую литературу. Журналы входят в перечень ВАК.

→ *Информационный ресурс:* Информационно-аналитический журнал «Дети в информационном обществе» Фонда развития Интернета.

Ссылка: http://www.fid.su/publishing/journal

Комментарий: журнал «Дети в информационном обществе» посвящен темам социализации, образования, личностного и духовного развития детей в эпоху глобальных социально-культурных перемен, вызванных бурным ростом информационно-коммуникационных технологий. Издание ориентировано на тех, кто профессионально работает со школьниками и детьми дошкольного возраста.

→ *Информационный ресурс:* Страница сайта ПАО «МТС» «Безопасность – это просто».

Ссылка: http://www.safety.mts.ru/ru/

Комментарий: страница сайта ПАО «МТС», посвященная вопросам безопасности. На странице можно найти информацию об интернет-угрозах и способах борьбы с ними, есть раздел, посвященный интернет-безопасности детей.

→ *Информационный ресурс:* Компэду.

Ссылка: https://compedu.ru/publication/informatika/

Комментарий: сайт дистанционных олимпиад для учителей и школьников. Представлены также различные материалы для учителя информатики: уроки, тесты, конспекты, презентации, планы, мероприятия и др.

→ *Информационный ресурс:* Социальная сеть работников образования.

Ссылка: https://nsportal.ru/

Комментарий: на сайте представлена библиотека методических материалов, структурированная по уровням образования, где можно найти различные материалы для проведения занятий по формированию цифровой грамотности и, в частности, навыков безопасного поведения в сети Интернет.

→ *Информационный ресурс:* Сайт международного конгресса конференций «Информационные технологии в образовании».

Ссылка: https://ito.evnts.pw/

Комментарий: на сайте размещена систематизированная, структурированная информация о деловых мероприятиях разной тематической направленности, включая интернет-безопасность.

→ *Информационный ресурс:* Федеральная программа безопасного детского интернета «Гогуль».

Ссылка: http://gogul.tv/

Комментарий: Детский интернет-браузер Гогуль – это программа для ограничения доступа в интернет и фильтрации содержимого веб-ресурсов, для обеспечения безопасности ребёнка и родительского контроля детского сёрфинга по сети. Безопасность ребенка в интернете обеспечивается за счет каталога детских сайтов, проверенных педагогами и психологами, и насчитывающего тысячи детских интернет-сайтов. Гогуль ведет статистику посещенных сайтов для родительского контроля интернет-сёрфинга ребенка, а также может ограничивать время пребывания детей в интернете.

СПИСОК РЕКОМЕНДУЕМОЙ ЛИТЕРАТУРЫ

Асмолов А.Г. Оптика просвещения: социокультурные перспективы. — М.: «Просвещение», 2012. С. 447.

Асмолов А.Г., Семенов А.Л., Уваров А.Ю. Российская школа и новые информационные технологии: взгляд в будущее десятилетие. – М., 2010. С. 84

Белинская Е.П. Совладание как социально-психологическая проблема / Е.П. Белинская. - Психологические исследования: электронный научный журнал. - 2009. - № 1(3). - Электронный ресурс. - Режим доступа: http://psystudy.ru.

Васильева М.Г. Интернет-ресурсы в физкультурном образовании / М.Г. Васильева // Физкультурное образование Сибири: научно-методический журнал. – № 2. – Омск, 2014. С. 7–11.

Данилов О.Е. Роль информационно-коммуникационных технологий в современном процессе обучения / О.Е. Данилов // Молодой ученый. – 2013. – № 12. С. 448–451.

Ливингстон С., Блум-Росс А. Только не Инстаграм! // Дети в информационном обществе. – 2016. – № 25. – С. 30–35.

Никольская И.М., Грановская Р.М. Психологическая защита у детей. – СПб: Речь, 2006. С. 342

Полезный и безопасный интернет. Правила безопасного использования интернета для детей младшего школьного возраста: практическое пособие / под ред. Г.У. Солдатовой; 3-е изд., перераб. и доп. – М.: Федеральный институт развития образования, 2017. С. 64

Практическая психология безопасности: управление персональными данными в интернете / Г.У. Солдатова, А.А. Приезжева, О.И. Олькина, В.Н. Шляпников. – Федеральный институт развития образования Москва, 2016. С. 204

Солдатова Г.В., Зотова Е.Ю., Чекалина А.И., Гостимская О.С. Пойманные одной сетью: социально-психологическое исследование представлений детей и взрослых об интернете / Под ред. Г.В. Солдатовой. – М., 2011. С. 176

Солдатова Г.У., Олькина О.И. 100 друзей. Круг общения подростков в социальных сетях // Дети в информационном обществе. – 2016. – № 24. – С. 24–33.

Солдатова Г.У., Рассказова Е.И. Модели передачи опыта между поколениями при освоении и использовании интернета // Вопросы психологии. – 2015. – № 2. – С. 56–66.

Солдатова Г.У., Рассказова Е.И. Психологические модели российских подростков и родителей. // Национальный психологический журнал. – 2014. – 2(14). С. 27-35.

Солдатова Г.У., Шляпников В.Н. Игры, мультики, учёба // Дети в информационном обществе. – 2014. – № 17. С. 44–47.

Солдатова Г.У., Шляпников В.Н., Журина М.А. Эволюция онлайн-рисков: итоги пятилетней работы линии помощи Дети онлайн // Консультативная психология и психотерапия. – 2015. – Т. 23, № 3. С. 50–66.

Социальная компетентность классного руководителя: режиссура совместных действий / под. редакцией А.Г. Асмолова, Г.У. Солдатовой. - Москва: Смысл, 2006.

Холловэй Д. От 0 до 8 // Дети в информационном обществе. – 2014. – № 17. С. 24-33.

Цифровая компетентность подростков и родителей. Результаты всероссийского исследования / Г.У. Солдатова, Т.А. Нестик, Е.И. Рассказова, Е.Ю. Зотова. — М.: Фонд Развития Интернет, 2013. С. 144

Gilster P. Digital Literacy. N.Y.: Wiley Computer Publishing, 1997.

Griffiths M. The role of context in online gaming excess and addiction: some case study evidence // International Journ. of Mental Health and Addiction. - 2010. - № 8. P. 119-125.

Livingstone, S., Haddon, L., Görzig, A., & Ólafsson, K. (2011a). Risks and safety on the internet: The perspective of European children. Full findings. London: EU Kids Online, LSE.

Marriage K., Cummins R.A. Subjective quality of life and self-esteem in children: the role of primary and secondary control in coping with everyday stress // Social Indicators Research. - 2004. - Vol. 66. - N 1-2. P. 107-122.

Martin A., Madigan D. (Eds.). Digital literacies for learning. - L.: Facet, 2006.

Mossberger K., Tolbert C.J., McNeal R.S. Digital citizenship: The internet, society, and participation. - Cambridge, MA: MIT Press, 2008.

Subrahmanyam K., Smahel D. Digital Youth, Advancing Responsible Adolescent Development, Springer Science+Business Media, LLC, 2011.