Методические рекомендации для педагогов по организации и проведению просветительских мероприятий по вопросам обеспечения информационной безопасности детей и подростков, профилактики компьютерной зависимости у обучающихся

Проблема обеспечения информационной безопасности детей в сети Интернет становится все более актуальной в связи с постоянным ростом несовершеннолетних пользователей.

Современные школьники имеют гораздо более широкий доступ к различным компьютерным технологиям с выходом во всемирную паутину, а соответственно и доступ к большим объемам различной информации, чем предыдущие поколения.

Для многих школьников Российской Федерации, и в том числе Донецкой Народной Республики, Интернет становится информационной средой, без которой они не представляют себе жизнь. Этому также способствовал длительный период дистанционного обучения, на который были вынуждены перейти образовательные организации республики.

Помимо информационных материалов, необходимых для использования в образовательном процессе, в сети Интернет содержатся огромные массивы информации, запрещенной для детей, которая может нанести вред их физическому и психическому здоровью.

В связи с этим задача взрослых, влияющих на жизнь ребенка (педагоги, родители, законные представители), помочь обучающимся усвоить правила пользования Интернетом, знать источники опасности, которые таит в себе всемирная паутина, и первоочередные шаги для обеспечения безопасности.

Цель методических рекомендаций: оказать методическую помощь педагогическим работникам образовательных организаций основного общего образования и среднего общего образования при организации работы с обучающимися и их родителями (законными представителями) по информационной безопасности, которая сможет предупредить угрозы и сделать работу детей и подростков в сети Интернете полезной и безопасной.

НОРМАТИВНЫЕ ПРАВОВЫЕ АКТЫ ПО ОБЕСПЕЧЕНИЮ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

В соответствии с Конституцией Российской Федерации дети являются важнейшей ценностью государства и общества. Государство создает условия, способствующие их всестороннему духовному, нравственному, интеллектуальному и физическому развитию, воспитанию патриотизма, гражданственности и уважения к старшим.

Указом Президента РФ от 05.12.2016 № 646 утверждена Доктрина информационной безопасности Российской Федерации, представляющая собой изложение систем официальных взглядов на место РФ в современном мире информационных технологий, на угрозы суверенитету страны, а также средств, которые используются для выстраивания взаимодействия между государствами в цифровом обществе.

Согласно Доктрине, национальные интересы в информационной сфере включают обеспечение и защиту конституционных прав и свобод человека и гражданина в части, касающейся получения и использования информации, неприкосновенности частной жизни при использовании информационных технологий, обеспечение информационной поддержки демократических институтов, механизмов взаимодействия государства и гражданского

общества, а также применение информационных технологий в интересах сохранения культурных, исторических и духовно-нравственных ценностей многонационального народа РФ.

Одним из главных положений Доктрины в первую очередь нужно выделить обеспечение защиты прав граждан от всевозможных посягательств с задействованием информационных средств, защиты от вторжения в частную жизнь, посягательств на денежные средства, хранящиеся на банковских карточках и другое электронное имущество.

Проблема информационной безопасности детей нашла свое отражение Федеральном законе от 29.12.2010 N 436-ФЗ "О защите детей от информации, причиняющей вред их здоровью и развитию" (с изменениями, действует редакция от 28.04.2023), регулирующем отношения, связанные с защитой детей от информации, причиняющей вред их здоровью и (или) развитию, в том числе от такой информации, содержащейся в информационной продукции. К такой информации относится пропаганда вредных привычек, оправдание детской жесткости, отрицание семейных ценностей.

В соответствии со статьей 5 N 436-ФЗ к информации, запрещенной для распространения среди детей, относится информация:

– побуждающая детей к совершению действий, представляющих угрозу их жизни и (или) здоровью, в том числе к причинению вреда своему здоровью, самоубийству, либо жизни и (или) здоровью иных лиц, либо направленная на склонение или иное вовлечение детей в совершение таких действий;

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

– обосновывающая или оправдывающая допустимость насилия и (или) жестокости либо побуждающая осуществлять насильственные действия по отношению к людям или животным;

– содержащая изображение или описание сексуального насилия;

– отрицающая семейные ценности и формирующая неуважение к родителям и (или) другим членам семьи;

– пропагандирующая либо демонстрирующая нетрадиционные сексуальные отношения и (или) предпочтения, способная вызвать у детей желание сменить пол;

– оправдывающая противоправное поведение;

– содержащая нецензурную брань;

– содержащая информацию порнографического характера;

– содержащаяся в информационной продукции, произведенной иностранным агентом.

В соответствии со ст.6 № 436-ФЗ, ограничения информационной продукции распространяются на разные возрастные группы детей:

– информационная продукция для детей, не достигших возраста 6 лет;

– информационная продукция для детей, достигших возраста 6 лет;

– информационная продукция для детей, достигших возраста 12 лет;

– информационная продукция для детей, достигших возраста 16 лет;

– информационная продукция, запрещенная для детей.

Проблема защиты детей от информации напрямую связана с темой образования. Формирование у обучающихся умений работать с информацией и обеспечивать ее

безопасность, является важной задачей образования. Ответственность образовательной организации по вопросу обеспечения информационной безопасности детей закреплена в Федеральном законе от 29.12.2012 №273-ФЗ «Об образовании в Российской Федерации» (с изменениями, действует редакция от 25.12.2023), а именно требования к созданию необходимых условий для охраны и укрепления здоровья обучающихся, на основании которых можно выделить задачи педагогического характера для организации мероприятий по информационной безопасности:

– формирование у обучающихся устойчивого убеждения в использовании информационных ресурсов;

– формирования устойчивых поведенческих навыков в сфере информационной безопасности;

– развитие у обучающихся способности распознать и противостоять негативной информации в Интернет-пространстве и СМИ, через обучение способам защиты от вредной информации.

Также обеспечение информационной безопасности в РФ регламентировано следующими нормативно-правовыми документами:

1. Федеральный закон от 27.07.2006 № 149-ФЗ «Об информации, информационных технологиях и о защите информации» (с изменениями, действует редакция от 12.12.2023) определяет механизм физического ограничения доступа к запрещенной информации в сети Интернет, предусматривающий создание федерального реестра сетевых адресов, доменных имен и указателей страниц, содержащих информацию, распространение которой в России запрещено - Единый реестр доменных имен. Доступ к сайту, внесенному в Единый реестр, блокируется оператором связи, предоставляющим доступ к сети Интернет;

2. Федеральный закон от 25.07.2002 № 114-ФЗ «О противодействии экстремистской деятельности» (с изменениями, действует редакция от 28.12.2022) возлагает на Минюст России функции по ведению, опубликованию и размещению в сети Интернет федерального списка экстремистских материалов. Информационные материалы признаются экстремистскими федеральным судом по месту их обнаружения, распространения или нахождения организации, осуществившей производство таких материалов. Федеральный список экстремистских материалов формируется на основании поступающих в Минюст России копий вступивших в законную силу решений судов о признании информационных материалов экстремистскими.

3. Федеральный закон от 27.07.2006 № 152-ФЗ «О персональных данных» (с изменениями, действует редакция от 06.02.2023) устанавливает, что персональные данные являются любой информацией, относящаяся к прямо или косвенно определенному или определяемому физическому лицу. Юридические и физические лица, в соответствии со своими полномочиями владеющие информацией о гражданах, получающие и использующие ее, несут ответственность в соответствии с законодательством РФ за нарушение режима защиты, обработки и порядка использования этой информации, в частности предусмотрена административная ответственность. Основные виды угроз конфиденциальности информации: разглашение, утечка, несанкционированный доступ.

Письмом Минобрнауки России от 28.04.2014 N ДЛ-115/03 "О направлении методических материалов для обеспечения информационной безопасности детей при использовании ресурсов сети Интернет" был сформирован перечень информации, не соответствующей задачам образования:

1. Компьютерные игры, за исключением соответствующих задачам образования: информационная продукция (в том числе сайты, форумы, доски объявлений, страницы социальных сетей, чаты в сети Интернет) по тематике компьютерных игр, не соответствующая задачам образования, такая как порталы браузерных игр, массовые многопользовательские онлайн ролевые игры.

2. Банки рефератов, эссе, дипломных работ, за исключением соответствующих задачам образования: информационная продукция, представляющая собой банки готовых рефератов, эссе, дипломных работ, за исключением печатных и электронных образовательных и информационных ресурсов, создаваемых в организациях, осуществляющих образовательную деятельность.

3. Онлайн-казино и тотализаторы: информационная продукция, содержащая информацию об электронных казино, тотализаторах, играх на деньги.

4. Мошеннические сайты: сайты, навязывающие платные услуги на базе СМС-платежей, сайты, обманным путем собирающие личную информацию (фишинг).

5. Магия, колдовство, чародейство, ясновидящие, приворот по фото, теургия, волшебство, некромантия, тоталитарные секты: информационная продукция, оказывающая психологическое воздействие на детей, при котором человек обращается к тайным силам с целью влияния на события, а также реального или кажущегося воздействия на состояние.

Концепция информационной безопасности детей в Российской Федерации утверждена Распоряжением Правительства РФ от 28.04.2023 № 1105-Р (далее - Концепция ИБ), в которой отмечается, что деструктивное информационное воздействие способствует развитию формирования у детей и подростков неправильного восприятия традиционных российских духовно-нравственных ценностей, провоцирующего "психологический слом", следствием которого могут стать как депрессивное состояние, так и проявление девиантного поведения, повышенной агрессии к окружающим.

В Концепции ИБ приведены принципы государственной политики в области обеспечения информационной безопасности детей, среди которых можно выделить следующие:

– укрепление ведущей роли государства в обеспечении информационной безопасности детей;

– сохранение и укрепление традиционных ценностей, противодействие распространению деструктивной информации;

– ответственность родителей (законных представителей) за воспитание и развитие своих детей, включая заботу о здоровье, физическом, психическом, духовном и нравственном развитии своих детей;

– приоритетность прав и обязанностей родителей (законных представителей) в обеспечении информационной безопасности детей;

– необходимость формирования у детей умения ориентироваться в современной информационной среде;

– воспитание у детей навыков самостоятельного и критического мышления;

– обучение детей вопросам информационной безопасности;

– поддержка творческой деятельности детей в целях их самореализации в информационной среде;

– безопасность использования интернет-технологий в образовательных организациях и местах, доступных для детей и др.

Вопросы информационной безопасности детей и подростков отражены в Концепции развития системы профилактики безнадзорности и правонарушений несовершеннолетних на период до 2025 года, утвержденной Распоряжением Правительства РФ от 22.03.2017 № 520-р, которая представляет собой систему взглядов, принципов и оснований в профилактической работе с несовершеннолетними, предусматривает основные направления, формы и методы совершенствования и развития системы профилактики безнадзорности и правонарушений несовершеннолетних. В частности в Концепции уделено особое внимание таким антиобщественным действиям, как запугивание, травля (буллинг) ребенка со стороны одноклассников, распространение лживой, порочащей ребенка информации в социальных сетях, которые нередко воспринимаются как норма не только детьми, совершающими противоправные поступки, но и жертвами такого поведения. Отмечается, что имеют место случаи размещения в информационно-телекоммуникационной сети Интернет видеосюжетов со сценами побоев, истязаний и иных насильственных действий в отношении малолетних детей и подростков, что значительно усугубляет психологические травмы жертв. Кроме того, сам факт распространения в информационно-телекоммуникационных сетях подобных видеоматериалов способствует культивированию насилия среди несовершеннолетних и провоцирует их на подобные съемки.

В Концепции среди основных направлений развития системы профилактики безнадзорности и правонарушений несовершеннолетних включена необходимость преобразования в сферах массовой информации, рекламной и издательской деятельности, формирования информационного пространства, обеспечивающего развитие нравственных ценностей, законопослушного поведения.

Федеральные государственные образовательные стандарты основного общего образования и среднего общего образования в части результатов освоения основной образовательной программы также подчеркивают важность обучения детей навыкам и знаниям обучающихся в сфере информационной безопасности.

ТЕОРЕТИЧЕСКИЕ АСПЕКТЫ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

Ключевые понятия в области информационной безопасности:

1. ***Информационная безопасность образовательной организации*** - практика предотвращения несанкционированного доступа, использования, раскрытия, искажения, изменения, исследования, записи или уничтожения информации, а также защищенность информационных ресурсов от вредоносных воздействий.

При этом к вредоносным воздействиям на образовательную организацию относятся:

– попытки проникновения злоумышленников;

– ошибки персонала;

– выход из строя аппаратных и программных средств;

– стихийные бедствия и др.

2. Информационная безопасность общества – состояние защищенности информационной среды общества, обеспечивающее ее формирование и развитие в интересах граждан, организаций, государства; безопасность информационного обеспечения жизненно-важных интересов личности.

Нарушение информационной безопасности личности (как элемента общества) может возникнуть:

– в случае негативного информационного воздействия;

– в случае дефицита или отсутствия необходимой информации.

3. Информационная безопасность детей – это состояние защищенности детей, при котором отсутствует риск, связанный с причинением информацией, в том числе распространяемой в сети Интернет, вреда их здоровью, физическому, психическому, духовному и нравственному развитию. Такую защищенность ребенку могут и должны обеспечить, прежде всего, значимые взрослые.

4. Информационная грамотность – поиск, интерпретация, оценка различных источников информации, работа с видами учебных, деловых и научно-популярных текстов.

5. Информационная культура – совокупность материальных и духовных ценностей в области информации.

6. Медиаграмотность – это грамотное использование детьми и их преподавателями инструментов, обеспечивающих доступ к информации, развитие критического анализа содержания информации и привития коммуникативных навыков, содействие профессиональной подготовке детей и их педагогов в целях позитивного и ответственного использования ими информационных и коммуникационных технологий и услуг.

7. Информационный иммунитет – способность личности отражать негативное влияние информационной среды, выражающаяся в умении выявлять информационные угрозы, определять степень их опасности и умело противостоять им; адекватное восприятие и оценка информации, ее критическое осмысление на основе нравственных и культурных ценностей.

По мере своего взросления ребенок постигает окружающий мир путем поглощения различной информации. При этом его развитие определено возрастными психологическими особенностями (достижениями личностного и познавательного развития - уровнем развития интеллекта), темпераментными особенностями, ценностями, мотивами. Личностные и интеллектуальные компетенции ребенка изменяются, развиваются, дают возможность справиться с любыми деструкциями социальной среды, но часто сами недостаточны или ограничены возрастными границами и аллюзиями.

Следовательно, информационная безопасность детей выражается в двух аспектах:

– защита от вредного воздействия информационной среды;

– развитие на основе системы условий, обеспечивающих позитивную социализацию и индивидуализацию ребенка.

Таким образом, ***информационная безопасность детей*** может быть определена как защищенность ребенка от дестабилизирующего воздействия информационной продукции на здоровье и психическое, духовное, нравственное развитие, как создание условий информационной среды для позитивной социализации и индивидуализации личности, оптимального социального, личностного, познавательного и физического развития, сохранения соматического, психического и психологического здоровья и благополучия, формирования позитивного мировосприятия.

Как было отмечено ранее, в законе № 436-ФЗ для разных возрастные группы детей установлены различные ограничения информационной продукции.

Информационная продукция, допустимая для детей, достигших возраста 6+ лет:

– кратковременные и ненатуралистичные изображения или описание заболеваний (за исключением тяжелых) или их последствий в форме, не унижающей достоинства человека,

– ненатуралистические изображения несчастного случая, аварии, катастрофы либо насильственной смерти без демонстрации их последствий, которые могут вызвать у детей страх, ужас или панику;

– не побуждающие к совершению антиобщественных действий и (или) преступлений, эпизодические изображения или описание этих действий и(или) преступлений при условии, что не обосновывается и не оправдывается их допустимости и выражается отрицательное, осуждающее отношение к лицу, их совершающим.

Возраст, с 6 до 12 лет - широкий спектр социально-психологических отклонений в значимых для ребенка сферах жизнедеятельности и основных расстройств возрастного психического развития на фоне неправильного восприятия и потребления неконтролируемого количества деструктивной информации:

1. В сфере семьи:

– стрессы у родителей и стойкие внутрисемейные конфликты с вовлечение в них ребенка;

– противопоставления родительских или семейных ценностей ценностям ребенка.

2. В сфере школы:

– школьная неуспеваемость и конфликты с учителем;

– высокая частота случаев смены школы при конфликтных ситуациях;

– непринятие одноклассниками.

Информационная продукция для детей, достигших возраста 12+ лет:

– эпизодические изображение или описание жестокости и (или) насилия (за исключением сексуального насилия) без натуралистического показа процесса лишения жизни или нанесения увечий при условии, что выражается в сострадании к жертве и (или) отрицательное, осуждающее отношение к жестокости, насилию (за исключением насилия, применяемого в случаях защиты прав граждан и охраняемых законом интересов общества или государства);

– изображение или описание, не побуждающие к совершению антиобщественных действий (в том числе к потреблению алкогольной и спиртосодержащей продукции, пива и напитков, изготавливаемых на его основе, участию в азартных играх, занятию бродяжничеством или попрошайничеством), эпизодическое упоминание (без демонстрации) наркотических средств, психотропных и (или) одурманивающих веществ, табачных изделий при условии, что не обосновывается допустимость антиобщественных действий, выражается отрицательное, осуждающее отношение к ним и содержится указание на опасность потребления указанных продукции, средств, веществ, изделий);

– не эксплуатирующие интереса к сексу и не носящие возбуждающего или оскорбительного характера эпизодические ненатуралистические изображение или описание половых отношений между мужчиной и женщиной, за исключением изображения или описания действий сексуального характера.

Информация с возрастным ограничением для детей, достигших возраста шестнадцати лет:

– изображение или описание несчастного случая, аварии катастрофы, заболевания без натуралистического показа их последствий, которые могут вызвать у детей страх, ужас или панику;

– изображение или описание жестокости и насилия (за исключением сексуального насилия) без натуралистического показа лишения жизни или нанесения увечий при условии, что выражается сострадание к жертве и отрицательное, осуждающее отношение к жестокости, насилию (за исключением насилия, применяемого в случаях защиты прав граждан и охраняемых законов интересов общества или государства);

– информация о наркотических средствах или о психотропных и (или) одурманивающих веществ (без их демонстрации), об опасных последствиях их потребления с демонстрацией таких случаев при условии, что выражается отрицательное или осуждающее отношение к потреблению таких средств или веществ и содержится указание на опасность их потребления;

– отдельные бранные слова и (или) выражения, не относящиеся к нецензурной брани;

– не эксплуатирующие интереса к сексу и не носящие оскорбительного характера изображения или описание половых отношений между мужчиной и женщиной, за исключением изображения или описания действий сексуального характера.

В подростковом возрасте, начиная с 12 лет, существенным образом изменяется нравственное развитие школьника. Усвоение ребенком нравственного образца происходит тогда, когда он совершает реальные нравственные поступки в значимых для него ситуациях.

Негативная информация в этом периоде может нанести значительный ущерб развитию личности, именно поэтому подросткам необходимо оказать нужное педагогическое влияние через реальное взаимодействие, потому что вследствие недостаточной обобщенности нравственного опыта нравственные убеждения подрастающего поколения находятся в неустойчивом состоянии.

Подростковый возраст − это период изменений и в организме, и в психике человека. Меняется тело, меняется восприятие мира, отношения к себе и окружающим. В этот период ребенок становится особенно восприимчивым и беззащитным перед всякого рода деструктивными влияниями. Понимание и поддержка от окружающих его взрослых (педагогов, родителей) становится для него спасительным кругом и твердой опорой для гармоничного развития и успешной социализации.

ОСНОВНЫЕ УГРОЗЫ ДЛЯ ДЕТЕЙ В СЕТИ ИНТЕРНЕТ

Дети и подростки – активные пользователи интернета как в мире, так в РФ.

Доступ несовершеннолетних к сайтам в сети Интернет дает им возможность изучать образовательный контент, общаться с ровесниками, самостоятельно обучаться, узнавать о проводимых конкурсах, олимпиадах, принимая в них участие, и использовать сеть Интернет в качестве источника для собственного развития.

Однако использование сети Интернет вместе с возможностями несет и различные риски.

В Концепции ИБ приведены риски, которым подвержены дети в области виртуальной коммуникации дети:

– стать жертвой компьютерного мошенничества и вымогательства;

– вовлечение в сексуальную эксплуатацию, террористическую и экстремистскую деятельность;

– распространение наркотических средств, психотропных веществ и их прекурсоров, аналогов наркотических средств и психотропных веществ и новых потенциально опасных психотропных веществ посредством игровых активностей;

– вовлечение в сообщества с нарушением общепринятых норм морали;

– прочтение детьми информации, вредящей их мировоззрению и психотическому состоянию.

Современные дети, в отличие от предыдущего поколения, имеют более широкий доступ к средствам компьютерной техники (планшеты, мобильные телефоны, компьютеры с подключенным домашним, мобильным интернетом или точки доступа по wi-fi в

общественных местах). При этом многократно возросла нагрузка на нервную систему подростка, а перспектива остаться вне информационного потока вызывает сильную тревогу.

Опасности для детей и подростков в сети Интернет:

1. Вовлечение в опасные группы и движения

В соответствии с Концепцией ИБ, на сегодняшний день широкое распространение в цифровой среде получили деструктивные молодежные субкультуры, включая движения, связанные с вооруженным нападением на образовательные организации, популяризацией деятельности криминальных сообществ, продвижением преступных и антиобщественных действий, в том числе агрессивного, насильственного, суицидального, экстремального и экстремистского характера.

Все большее распространение получает задействование сетевых платформ и мессенджеров для вовлечения детей в несогласованные публичные мероприятия (включая протестные акции), поскольку несовершеннолетние не только легче поддаются идеологическому и психологическому воздействию, но и при определенных обстоятельствах не подлежат уголовной ответственности.

Вовлечение подростков в группы деструктивной направленности очень часто происходит через Интернет:

– социальные сети и информационные порталы («ВКонтакте»; «Фейсбук»*, «Инстаграм»* (*запрещены на территории Российской Федерации) и т.п.);

– Интернет-сообщества, тематические форумы, шок-контент (например, «Привет со дна», «Группа смерти» и др.);

– Интернет-игры (например, «Большая игра. Сломай систему!» и др.).

Общие маркеры вовлечения обучающихся в деструктивные группы:

– изменение внешности;

– изменение эмоционального состояния и его неустойчивость;

– преобладание в мировоззрении обучающихся идей неравенства, дискриминации, возмездия и наказания за несправедливое отношению;

– агрессивное поведение;

– использование сленга, относящегося определенной деструктивной идеологии;

– смена привычного образа жизни;

– безразличие к учебной, групповой и общественно-полезной деятельности;

– скрытность в отношении ежедневной занятости и планов;

– систематические пропуски учебных занятий по неуважительной причине.

Общие маркеры вовлечения обучающихся в деструктивные сообщества сети Интернет:

– резкое изменение данных личного профиля в социальных сетях;

– подписка на группы и сообщества, посвященные деструктивной идеологии или движению;

– публикация и репостинг материалов, отражающих содержание идей деструктивного сообщества (группы);

– публикация статусов, выражающих агрессию или содержащих отсылку к деструктивному движению;

– новые «друзья» в социальных сетях, разделяющие интерес ребенка к деструктивной идеологии («понимающие» его);

– ограничение доступа всех близких к личному Интернет – аккаунту.

Профилактическая работа с обучающимися по вопросам избегания вовлечения в опасные группы и движения:

– социально-педагогическая диагностика обучающихся;

– психологическая диагностика особенностей психоэмоционального состояния и личностных особенностей обучающихся;

– проведение разнообразных дискуссий, диспутов с несовершеннолетними;

– проведение деловых игр с целью выявления интересных и социально-значимых занятий;

– проведение психологических тренингов, циклов занятий, направленных на формирование и развитие толерантности;

– вовлечение в разнообразную организованную досуговую деятельность с учётом индивидуальных особенностей, способностей и потребностей обучающихся;

– вовлечение в детские и подростковые социальные проекты, направленные на включение школьников в социально-ориентированное творчество, на развитие их гражданской ответственности перед окружающим миром;

– межведомственное взаимодействие с субъектами профилактики.

2. Кибербуллинг

Кибербуллинг – различные формы травли, где агрессор и жертва встречаются в сети Интернет. Чаще всего пострадавшими становятся дети и подростки как самая уязвимая категория пользователей. Подросток, ставший объектом повышенного негативного внимания, испытывает на себе все «прелести» буллинга – уничижительные комментарии, оскорбления в сообщениях через мессенджеры, высмеивание в группах социальных сетей.

Механизмы травли в реальности и травли в сети «интернет» похожи, но кибербуллинг опаснее тем, что может происходить круглосуточно, от него не скроешься и не уйдешь домой.

В социальных сетях легко привлечь к процессу кибербуллинга большое количество последователей, распространив пост соответствующего содержания. Современным подросткам достаточно бросить клич в аккаунте, разместить фото и контакты объекта травли, регулярно поддерживать негативное отношение к нему записями на стене и так далее. Помимо прямых оскорблений в адрес жертвы, формой буллинга могут быть выложенные на всеобщее обозрение личные фото, фрагменты переписок, мемы, созданные на основе изображения человека, и др.

Подростковый кибербуллинг особенно опасен тем, что его инициаторы в силу возраста не способны оценить, какой вред могут нанести их действия. То, что агрессивно настроенным школьникам представляется невинной шалостью, нередко становится причиной трагических и даже летальных исходов.

Методы борьбы с кибербуллингом:

– игнорировать нападки – следует объяснить обучающимся необходимость сдерживать эмоции, не вступать в перепалку с человеком, который явно хочет спровоцировать на ответную грубость;

– не винить себя - многие несовершеннолетние склонны искать причину агрессивного поведения оппонента в себе: что я не так сказал, чем я вызвал волну негатива? Следует объяснить обучающимся, что лично они тут ни при чем – пользователю-агрессору все равно, с кем затеять свару;

– исключить вероятность общения – необходимо создать условия, при которых инициатор кибербуллинга не сможет продолжать свои действия: внести его в черные списки,

поставить запрет на поступление звонков и сообщений с его номера, а также писем с его электронных адресов;

– поделиться проблемой - кибербуллинг для подростков часто становится невыносимым испытанием, потому что им не с кем разделить свои переживания. Следует объяснить обучающимся, что если они не могут рассказать об этом родителям, можно позвонить в анонимную службу психологической поддержки: специалист внимательно выслушает, успокоит и даст дельный совет;

– бороться за свое спокойствие - травля в Интернете – явление распространенное, поэтому администрации соцсетей уже выработали алгоритм действий в случае жалоб на действия агрессивных пользователей. Они могут заблокировать профили, модерируют фотографии и посты, отслеживают появление комментариев с грубыми выражениями. Если дело дошло до угроз и клеветы, жертва кибербуллинга имеет все основания обратиться в полицию;

– дать отпор инициатору травли - агрессор рассчитывает, что жертва буллинга будет оправдываться, отвечать на его выпады колкостями, то есть поддаваться на провокации. Любая другая реакция собьет его с толку. Следует объяснить обучающимся, что лучше сразу заявить о своем намерении обратиться в суд с иском о клевете и угрозах – это может подействовать отрезвляюще;

– соблюдать цифровую диету - радикальный способ избавиться от виртуального преследования – полностью отказаться на время от социальных сетей. Следует объяснить обучающимся, что можно на время удалить приложения из телефона, переключиться на приятные дела в реальной жизни;

– изменить поведение в сети - если предыдущий способ не подходит, следует пересмотреть свое отношение к интернет-ресурсам: ограничеть количество пользователей, которым доступен размещаемый контент, удалить фотографии, которые могут спровоцировать травлю, и так далее;

– соблюдать правила цифровой грамотности - следует объяснить обучающимся необходимость защиты личного киберпространства при помощи регулярно сменяемых сложных паролей; не стоит переходить по сомнительным ссылкам или устанавливать непроверенные приложения.

3. *Домогательство, педофилия, завладение личной информацией или материалами с целью шантажа*

В настоящее время во всем мире наблюдается устойчивый рост преступлений связанных с сексуальным насилием, изготовлением и распространением порнографии, в том числе детской. Детская порнография стала более распространенной и доступной благодаря развитию СМИ и интернет-ресурсов.

Не только детям, но и взрослым следует внимательно оценивать изображения, которые они выкладывают в Сеть. Многие считают, что при общении в Интернете их никто не найдет и не увидит. Главная угроза в том, что приватные фотографии, видео или сообщения могут стать не столь приватными.

Случается, что социальные сети в корыстных целях используют злоумышленники:

– педофилы, которые, ищут новые жертвы, выдавая себя за сверстника, искать личной встречи;

– мошенники, которые пользуясь доверчивостью подростков, выведывают конфиденциальную информацию;

– злоумышленники могут получить доступ к облачному хранилищу, куда автоматически отправляется медиаконтент со смартфона;

– подросток может потерять смартфон или забыть его в общественном месте – подобравший телефон посторонний человек может получить доступ к медиафайлам;

– опасность невольно может исходить даже от знакомых людей - человек, которому отправили сообщение, может выложить фотографии в Интернет или переслать друзьям.

Попав в чужие руки, эротические фотографии или видео могут стать инструментом шантажа. Кроме того, подобные материалы, размещенные в социальных сетях, могут «перекочевать» на порносайты.

Педагогу следует обсудить с обучающимися, насколько может быть опасно отправлять личные, а тем более — интимные фото и видео, с помощью которых можно установить, где и с кем живет ребенок, где и в какое время часто бывает.

В рамках занятий по интернет-безопасности нужно объяснить обучающему основные правила:

– не публиковать в социальных сетях информацию, по которой твое местонахождение можно узнать (адрес, номер школы и др.);

– не нужно часто «чекиниться», то есть проставлять привязки к месту действия, выкладывая фотографии;

– держать страницу закрытой, в настройках разрешить отправку сообщений только друзьям и друзьям друзей;

– не идти на контакт с незнакомцами (и помнить, что даже за безобидной страницей сверстника может скрываться педофил);

– не встречаться в реальности с незнакомцами из социальных сетей; обсудить с ребенком возможные угрозы и опасности от встреч и онлайн-общения с незнакомцами и договориться о том, как он будет вести себя в той или иной ситуации;

– не высылать никому материалы, которые можно использовать для шантажа (например, пикантные фото, по которым тебя легко опознать);

– провести разъяснительную работу о том, что нельзя раскрывать информацию о себе незнакомым людям, доверять сведения личного характера человеку, которого никогда не видел вживую – разъяснить обучающимся, что в Интернете человек может представиться кем угодно;

– рекомендовать подросткам не рассказывать в Сети ничего такого, чего они могут стесняться;

– отказывать – нормально; не нужно бояться обидеть собеседника, если он просит сделать что-то неприятное для тебя;

– создавать сложные пароли, различные для каждой социальной сети и электронной почты. Хранить пароли в надежном месте. Менять их с периодичностью 2-3 месяца. Настроить двухэтапную аутентификацию;

– обращаться за помощью, если не справляешься с ситуацией. Как и во всех предыдущих ситуациях, крайне важно поддерживать атмосферу доверия в отношениях. Инструменты шантажа и манипуляции работают тогда, когда понимание того, что о ситуации кто-то узнает (родители, учителя, одноклассники), вызывает у подростка ужас.

4. Кража паролей/аккаунтов в социальных сетях или играх

Социальные сети и онлайн-игры стали настоящей пропиской современных детей.

В социальных сетях они заводят друзей, общаются, делятся информацией, выкладывают фото и видео.

В онлайн-играх дети уделяют своим виртуальным героям много времени, «прокачивают» их, скупают «игровой шмот» за реальные деньги, которые дают родители, и страшно переживают, если с их аккаунтом что-то случилось.

Воровство паролей в социальных сетях и онлайн-играх явление достаточно распространенное, как результат можно потерять аккаунт и деньги, имеющиеся на привязанной SIM-карте или карте банка.

Судя по уже существующей в сети Интернет информации, чаще всего жертвы (дети 6-14 лет) сами сообщают свой пароль злоумышленникам, или мошенник заманивает пользователя на фишинговую страницу, предлагая ввести пароль с целью получить дополнительно игровые бонусы или привязать различные «фишки» к своей странице «ВКонтакте». Как только ребенок вводит пароль, его аккаунт немедленно крадут, а с ним зачастую и все деньги, имеющиеся на SIM-карте.

В рамках занятий по интернет-безопасности можно объяснить обучающему как защитится от кражи личных данных:

– рассказать о типах почты, которую могут рассылать злоумышленники, включая рекламу кредитных карт, необъяснимые товары и уведомления о сборе средств;

– рассказать о важности сохранения личной информации, такой как фамилии, адреса и номера телефонов, в тайне при обмене информацией в интернете;

– информируйте детей о нежелательных мошенничествах по электронной почте, таких как «фишинговые» электронные письма, в которых запрашивается личная информация, объясните, что лучше сразу удалять мошеннические электронные письма такого рода;

– провести разъяснительную работу о том, что нельзя раскрывать информацию о себе незнакомым людям, отвечать на различные наводящие вопросы, переходить по заманчивым ссылкам.

5. Интернет-зависимость от социальных сетей, сетевых игр, «серфингом», онлайн-казино

Интернет-зависимость - навязчивое стремление использовать Интернет и избыточное пользование им, проведение большого количества времени в сети.

Существует несколько видов интернет зависимостей:

– серфинг – бесцельное листание страниц, переходы по разным ссылкам и чтение не нужной информации;

– игровая зависимость – постоянное зависание в сетевых играх;

– финансовая зависимость – присутствует постоянное желание что-то купить в интернет-магазине;

– азартность – частое участие в аукционах, лотереях, розыгрышах, азартных интернет играх;

– зависимость от общения – отличается большим количеством переписок, участие в чатах, форумах, слишком большое количество друзей и подписчиков в социальных сетях, с которыми ребенок даже не знаком;

– киберсексуальная зависимость – частое посещение сайтов с порнографическим контентом, просмотр роликов и фотографий сексуального характера, интимные переписки;

– зависимость от видео – просмотр большого количества фильмов через интернет, сериалов, видеороликов различной тематики. Часто зритель даже не может рассказать, о чем было просмотренное видео.

В последнее время интернет-зависимость все чаще наблюдается у детей и подростков. Основным симптомом является желание в любую свободную минуту зайти в интернет. Взгляд очень долго прикован к смартфону или много времени проводится за компьютером без определенной цели. Часто пропадает реакция на раздражающие факторы вокруг, а при попытке отвлечь от данного занятия проявляется агрессия или истерика.

Признаки интернет-зависимости у ребенка:

– ребенок проводит в глобальной сети больше свободного времени, чем прежде. Его тяжело оторвать от этого занятия;

– если забрать гаджет, он не знает, чем себя занять, у него резко ухудшается настроение и наблюдается упадок сил;

– у ребенка нарушается сон, он беспокойно спит ночью;

– у школьника снижается успеваемость в учёбе, он становится рассеянным и невнимательным;

– ребенок все время проводит в интернете, даже во время обеда или ужина;

– родные люди и друзья не радуют ребенка. Виртуальное общение вытесняет реальное. Ребенок не общается со сверстниками, не играет с друзьями, пропускает школу и секции, не ходит гулять. Он предпочитает проводить время у компьютера;

– перестает выполнять свои прямые обязанности по дому: не хочет выносить мусор, мыть посуду, убирать свои вещи в шкаф;

– наблюдаются нарушения режима дня, отсутствие аппетита;

– нестабильное настроение ребенка, частая смена настроения, скрытность;

– необходимость быть «онлайн» ежеминутно. Стремление регулярно проверять социальные сети и онлайн-игры;

– если ребенок остается без интернета, он становится агрессивным и его всё раздражает, может устроить истерику.

Признаки интернет-зависимости у подростков:

– во время нахождения в сети подросток чувствует радость, как только он оказывается в обстановке без Интернета – становится раздражительным и теряет интерес к окружению;

– редко выходит на улицу, все свободное время проводит дома в сети;

– подросток перестает общаться со своими сверстниками, предпочитает виртуальное общение;

– подросток ведет пассивный образ жизни, снижается двигательная активность;

– в школе появляются проблемы с успеваемостью, плохо выполняются домашние задания;

– все разговоры и мысли только о сайтах, которые он посещает;

– не посвящает родителей в свои интересы, может им врать, стремится получить желаемое любыми способами;

– ухудшается память и внимание, снижается здоровье (ухудшается зрение, появляются проблемы с позвоночником и желудком), перестает следить за собой, становится неряшливым;

– не реагирует на просьбы;

– подросток может красть деньги и ценные вещи из дома, могут появиться денежные долги;

– снижается самооценка, перестает верить в себя.

В рамках занятий по интернет-безопасности целью педагога (и родителей) при профилактике интернет-зависимости и компьютерной зависимости детей и подростков является повышение интереса к различным сферам современного досуга. Для достижения этой цели возможны следующие задачи:

– подготовка сознания ребенка к противодействию негативных воздействий компьютерных игр;

– помощь детям в осознании их образовательных потребностей и способах их удовлетворения с помощью компьютера (развлечение, снятие стресса, познание и др.);

– информированность школьников о воспитательных возможностях школы и внешкольных учреждений (секций, кружков);

– проведение внешкольных мероприятий (дискуссий, классных часов, игр) среди обучающихся на темы, связанные с компьютерной и интернет зависимостью (например, «Место компьютера и телевидения в моей жизни»).

6. Доступность материалов, предназначенных для старшей аудитории

Пожалуй, наиболее популярны у школьников и молодежи в настоящее время экранные медиа – телевидение, кинематограф, видео, в том числе транслируемые через интернет и компьютерный монитор. Именно с экрана начинается знакомство ребенка с медиамиром. Начиная с раннего возраста, дети неплохо запоминают увиденное на экране, становятся активными телезрителями (со своими предпочтениями и любимыми героями), а к поступлению в школу, как правило, уже осваивают азы компьютерной грамотности.

Особый эффект оказывает на молодежь столкновение с любым видом информационной продукции порнографического характера. Эти материалы не только стимулируют и меняют подростковое представление о сексуальных практиках, но и оказывают извращенное «образовательное» действие, служат в качестве модели и руководства к действию.

В настоящее время информационная безопасность детей при просмотре теле-, кино-, видеофильмов и программ регулируется также комплексом установленных законодательством РФ требований к содержанию аудиовизуальной информационной продукции, предназначенной для распространения среди разных возрастных групп несовершеннолетних.

Телевизионные передачи и фильмы, не предназначенные для детского просмотра, маркируются специальными значками, равноценными по величине логотипам каналов:

– для детей, не достигших возраста шести лет, - в виде цифры «0» и знака «плюс» (0+);

– для детей, достигших возраста шести лет, - в виде цифры «6» и знака «плюс» и (или) текстового предупреждения в виде словосочетания «для детей старше 6 лет»;

– для детей, достигших возраста двенадцати лет, - в виде цифры «12» и знака «плюс» и (или) текстового предупреждения виде словосочетания «для детей старше 12 лет»;

– для детей, достигших возраста шестнадцати лет, - в виде цифры «16» и знака «плюс» и (или) текстового предупреждения в виде словосочетания «для детей старше 16 лет»;

– для детей, - в виде цифры «18» и знака «плюс» и (или) текстового предупреждения в виде словосочетания «запрещено для детей».

Значок должен оставаться на экране минимум 8 секунд с момента начала передачи. Заменить его на текстовое или голосовое предупреждение телеканалы не могут.

7. Фишинг – получение доступа к логинам, паролям, банковским данным.

Цель данного вида мошенничества - получение ценных данных пользователей, которые могут быть проданы или использованы злоумышленниками для вредоносных целей, таких как вымогательство, похищение денег или кража личных данных.

Мошенники организуют рассылку сообщений по электронной почте якобы от имени банка со ссылками на поддельные страницы официальных сайтов. Вводя свои персональные данные (номера банковских карт, логины, пароли), жертва неосознанно передает конфиденциальную информацию мошенникам. А те, в свою очередь, используют сведения для завладения денежными средствами.

Аналогичные атаки осуществляются также через телефонные звонки (вишинг) и SMS-сообщения (смишинг).

Подсказки, которые помогут выявить фишинговое сообщение:

– общие или неофициальные приветствия - письма без персонализации (например, «Уважаемый клиент») и формальностей, должны вызвать подозрения;

– запрос личной информации – часто используется киберпреступниками, тогда как банки, финансовые учреждения и большинство онлайн-сервисов такие запросы направляют крайне редко;

– грамматические ошибки – орфографические ошибки и опечатки, а также необычные фразы часто могут означать опасность (но отсутствие ошибок не является доказательством легитимности);

– неожиданные сообщения – любой незапланированный контакт с банком должен вызывать подозрения;

– срочность – фишинговые сообщения часто побуждают к быстрым и менее продуманным действиям;

– предложение, от которого трудно отказаться – если содержание письма слишком хорошее, чтобы быть правдой, оно, вероятно, является фишинговым;

– подозрительный домен – будет ли американский или немецкий банк отправлять письмо с китайского домена.

Отдельным подвидом необходимо рассматривать мобильное мошенничество, которое в частности предполагает получение смс-сообщений с незнакомых номеров, которые могут содержать:

– ссылки на фишинговые или зараженные ресурсы;

– информацию о выигрышах, которых не существует;

– ложные просьбы о помощи;

– о переводе денег на сотовый, прямые просьбы о переводе денег;

– SMS из несуществующего банка;

– просьбы перезвонить на платный номер;

– требования выкупа;

–просьбы отправить СМС, которые активируют платные услуги и другую информацию.

Для предупреждения обучающихся о фишинг-мошенничестве можно:

– рассказать о специализированных интернет-ресурсах проверки сайтов на факты совершения мошеннических действий (например, https://довериевсети.рф/,

https://trustorg.com) и других сервисах контроля репутации сайта на предмет мошеннических действий;

– напомнить, что достоверный сайт обязательно содержит сведения об авторах и их контактные данные;

– обратить внимание на то, что нельзя вводить данные банковских карт на сомнительных сайтах интернет- магазинов (cvc/cvv-код, срок действия, номер карты);

– напомнить, что никому не стоит передавать или выкладывать в Сеть конфиденциальные данные (логин, пароль), свидетельство о рождении, паспортные данные, адрес прописки и фактического места жительства, слишком личные фотографии.

8. Нежелательные покупки, поддельные интернет-магазины.

В интернете существует большое количество поддельных магазинов, недобросовестных продавцов и лжепредпринимателей, которые могут обмануть, не предоставить товар или завладеть персональными данными для мошеннических действий. Покупать товар в сомнительном интернет-магазине довольно рискованно: в отличие от невиртуального магазина можно «потерять» карту, а не просто разовый платеж - если данные карты попадут в руки недобросовестных людей, они смогут присвоить всю сумму, которая находится на счету.

Основные типы афер с поддельными веб-сайтами:

– typosquatting - включает создание ложных, мошеннических или вредоносных веб-сайтов с веб-адресами, очень похожими на популярные сайты, в надежде, что пользователи будут переходить на них, набирая их случайно. Рекомендуется добавить часто используемые сайты в закладки, а не вводить их вручную в адресной строке;

– мышеловка - о метод, используемый интернет-маркетологами для «ловушки» пользователей на вредоносном сайте. Интернет-магазин может отключить вашу кнопку «назад» или засыпать вас несколькими всплывающими окнами. Через некоторое время вы сможете уйти, но в некоторых случаях у вас может не быть другого выбора, кроме как перезагрузить компьютер. Меры безопасности для защиты от "мышеловки" - отключить javascript в браузере или использовать надстройку для блокировки сценариев (NoScript - позволяет пользователям выбирать, какие сценарии запускать на каждой странице);

– pagejacking - происходит, когда поисковая система направляет пользователей на ложную копию популярного веб-сайта. Оказавшись там, пользователи обычно попадают на новые страницы, содержащие рекламу и предложения. В некоторых случаях эти сайты могут быть злыми или содержать непристойные материалы, такие как содержание ненависти или порнографию. Доступ к сайтам через "Избранное" или "Закладки" может помочь избежать неприятных последствий;

– фарминг - перенаправляет пользователей с законных сайтов на мошеннические магазины, которые отслеживают вводимую информацию, такую как номера кредитных карт, банковские данные, а также имена пользователей или пароли. Для этого рассылают вирус, который заставляет компьютеры связывать законное доменное имя с мошенническим веб-сайтом или атакуют сервер веб-сайта, так что каждый посетитель попадает на вредоносную версию сайта. Чтобы не стать жертвой фарминга, необходимо убедится, что вы посещаете защищенные веб-сайты (адрес веб-сайта должен начинаться с префикса https://). Также для предупреждения о недействительности сертификата веб-сайта (запись подлинности) следует установит программное обеспечение для обеспечения безопасности в Интернете (Kaspersky, McAffee или AVG).

Особенно рекомендуется обратить внимание и избегать сайты и сервисы:

– продающие технику, на которой отсутствует русификация. Это является одним из признаков контрабандного товара либо оборудование уже на заводе не планировалось поставлять в Россию;

– использующие для приема платежей электронные кошельки, поскольку такие сервисы предоставляют возможность принимать платежи сразу после регистрации, указав только электронную почту. E-mail нельзя отследить, что сказывается на отсутствие возможности установить личность продавца;

– которые не имеют пунктов самовывоза или своих офисов.

Для предупреждения обучающихся о мошенничестве при заказе через Интернет можно объяснить некоторые правила:

– обязательно нужно проверить интернет-магазин перед совершением покупки: на официальном сайте должны быть приведены сведения о правоустанавливающих документах (свидетельство о регистрации в налоговом органе, код ОКВЭД, ИНН, ОГРН), соглашение на использование и обработку персональных данных, адрес фактического расположения, данные о потребительских свойствах товара;

– следует доверять только известным и фирменным магазинам - в известных интернет-магазинах типа Wildberries, OZON и других есть все необходимое. С их помощью данные карты будут максимально защищены, потому что у крупных компаний отлаженная и безопасная система обработки;

– следует обращать внимание на адрес при входе на сайт обращать внимание на адрес - убедитесь, что вы действительно находитесь на amazon.com, а не на anazon.com или что в адресе после названия известного магазина нет какого либо окончания (например, «известный_магазин.ru-acw.xyz). Также нужно иметь ввиду, что доменные имена мошеннических магазинов, как правило, длинные и сложные, но в них присутствует имя известного бренда;

– не сообщать свои персональные данные (в том числе пароль от интернет-банкинга) и не переводить денежные средства лицам, которые не являются сторонами сайта;

– следует периодически проверять карту - если ее данные попадут в чужие руки, велика вероятность, что деньги «проскользнут» незамеченными - при небольшой сумме покупке или приобретении подарочных карт банк не заподозрит, что транзакция неавторизована, а вы будете частично ограблены;

– следует использовать только свой компьютер, планшет или телефон, к которым мало кто имеет доступ, при входе в интернет-банк или при совершении покупок в Интернете. Если все-таки нужен интернет-банкинг с чужого компьютера, не забывать удалить свои данные и не оставлять информацию, с которой вошли в систему - лучше всего открыть режим инкогнито или приватный режим браузера, после закрытия которого все данные и история страниц будут автоматически удалены. Чтобы безопасно выйти из интернет-банкинга по окончании работы обязательно воспользоваться кнопкой «Выйти»;

– следует избегать нереалистичных предложений – если сайт предлагает нереальные цены на новые модели мобильных телефонов или на новейшую дизайнерскую одежду – это мошенник. Конечно, часто будут встречаться скидки, но в этом случае необходимо наблюдать, на каком сайте вы находитесь, что мотивирует эту скидку и т. д.

Развитие интернет-торговли нередко вызывает у подростков желание не только купить, но и начать продавать товары. Некоторые школьники организуют группы продаж товаров из Китая, например, с площадок Aliexpress, некоторые выставляют на продажу свои поделки, творческие работы, личные вещи, размещают объявления об оказании услуг.

Посоветуйте им не продавать товары через неспециализированные интернет-сайты, социальные сети, рассылку рекламных сообщений. Для этого существуют специализированные сайты, например, https://www. avito.ru, https://youla.ru.

Обратите внимание обучающихся, что за регулярное распространение товаров и услуг, осуществляемое с нарушениями, можно быть обвиненным в незаконном предпринимательстве.

9. Информация о легком заработке.

Сейчас в сети Интернет набирают популярность объявления о легком и высоком заработке для подростков. Зачастую такая работа связана с вовлечением ребят в мошеннические или преступные схемы. Как правило, речь идет о распространении наркотических средств: подростки делают «закладки» в назначенных куратором местах, а затем их забирают клиенты. Стоимость такой подработки для школьников весьма привлекательна. Нередко подростки соглашаются, не догадываясь о характере доставляемого товара, однако иногда желание заработать перевешивает здравый смысл, и согласие участвовать в распространении наркотиков дается сознательно с расчетом остаться безнаказанными.

В рамках мероприятий по информационной безопасности обучающимся можно рекомендовать:

– анализировать любые «привлекательные» объявления на адекватность;

– всегда проверять информацию о работодателе, а проверив - настаивать на оформлении официальных трудовых отношений (с 14 лет) или договора гражданско-правового характера (с 15 лет) - если речь не идет ни о чем незаконном, работодатель должен согласиться;

– выяснять содержание и условия подработки до мелочей (почему так оценивается, что конкретно нужно делать, что нужно везти, какой товар доставлять);

– если что-то смущает – не стесняться спрашивать и выяснять любые подробности;

– всегда помнить, что за легкую работу ни один работодатель не будет расплачиваться крупной суммой денег;

– обращать внимание на предложения сделать что-то анонимно. Это один из маркеров того, что вас вовлекают в мошенническую схему.

10. Съемка фото и видео для размещения в сети Интернет, сопряженная с опасностью для жизни и здоровья

В последнее время среди интернет-пользователей набирает популярность фото- и видеосъемка как повседневных, так и ярких жизненных моментов, и размещение данного контента в сети Интернет. Некоторые примеры такого поведения детей:

– подросток становится невольным свидетелем вооруженного конфликта, стрельбы, взрыва и первым делом снимает происходящее на мобильный телефон. Вместо того чтобы предпринять необходимые меры безопасности (убежать, вызвать полицию), он снимает «уникальное видео» ради популярности в Сети, рискуя жизнью и здоровьем;

– выбор подростком опасных или экстремальных увлечений. Например, «руфинг» (прогулки по крышам), «скайуокинг» (покорение самых высоких точек в городе без специального снаряжения) или «зацепинг» (проезд вне салона электропоезда, трамвая – на крыше или подножке). Ради популярности в Интернете дети стремятся заснять свои «подвиги», что ведет к негативным последствиям. Такие увлечения сами по себе представляют смертельную опасность, а использование камеры только увеличивает риск оступиться, потерять равновесие или не заметить угрозу;

– стремление поразить интернет-друзей яркими или опасными фотографиями, сделанными в формате селфи. Как в России, так и в мире зафиксирована масса смертельных исходов при попытке сделать собственную фотографию в опасных местах, которые уже получили название «селфиубийства». Селфи на воде, на краях обрывов или скал, на железных и автомобильных дорогах, на крышах домов или промышленных объектов, вблизи линий электропередач могут привести к крайне негативным последствиям для жизни и здоровья ребенка.

Предотвратить подобные ситуации можно через формирование у обучающихся культуры личной безопасности. Она состоит в готовности защитить себя и окружающих от неблагоприятного воздействия, угроз и наступления нежелательных последствий. В рамках мероприятий по информационной безопасности обучающимся можно объяснить:

– объяснить, что при возникновении опасных ситуаций необходимо в первую очередь, позаботиться о безопасности себя и других людей, а затем вызвать полицию;

– провести беседу на тему опасных увлечений, при этом услышать от обучающегося аргументы в пользу его хобби. Главное — занять доброжелательную позицию со своей стороны, ненавязчиво предложить альтернативные виды деятельности, проходящие в безопасных условиях.

Важно не переусердствовать, но при этом донести до ребенка посыл, что он не безразличен вам, своей семье, близким и друзьям.

ПРОСВЕТИТЕЛЬСКИЕ МЕРОПРИЯТИЯ С ОБУЧАЮЩИМИСЯ «ОСНОВЫ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ»

Цель проведения мероприятий по вопросам обеспечения информационной безопасности детей и подростков, профилактики у них компьютерной зависимости – обеспечение информационной безопасности несовершеннолетних обучающихся путем привития им навыков ответственного и безопасного поведения в современной информационно-телекоммуникационной среде и при работе с компьютерной техникой.

Задачи мероприятий по вопросам обеспечения информационной безопасности обучающихся:

– информирование обучающихся о видах информации, способной причинить вред здоровью и развитию несовершеннолетних, запрещенной или ограниченной для распространения на территории РФ, а также о негативных последствиях распространения такой информации;

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

– ознакомление обучающихся с международными принципами и нормами, с нормативными правовыми актами РФ, регулирующими вопросы информационной безопасности несовершеннолетних;

– обучение детей и подростков правилам ответственного и безопасного пользования услугами Интернет и мобильной (сотовой) связи, другими электронными средствами связи и коммуникации, в том числе способам защиты от противоправных и иных общественно опасных посягательств в информационно-телекоммуникационных сетях, в частности, от таких способов разрушительного воздействия на психику детей, как кибербуллинг (жестокое

обращение с детьми в виртуальной среде) и буллицид (доведение до самоубийства путем психологического насилия);

– профилактика формирования у обучающихся Интернет-зависимости и игровой зависимости (игромании, гэмблинга);

– предупреждение совершения обучающимися правонарушений с использованием информационно-телекоммуникационных технологий.

Образовательная организация может организовать обучение своих обучающихся информационной безопасности путем:

– обращения внимания вопросам обеспечения информационной безопасности в рамках действующих в образовательной организации учебных дисциплин (в рамках курса «Информатика» и других предметных областей);

– внедрения в образовательную программу самостоятельной учебной дисциплины или увеличение количества учебных часов на изучение данной проблематики при изучении учебных предметов в рамках вариантовой части учебного плана образовательной программы;

– организации соответствующих мероприятий или обучения в рамках тематической внеурочной деятельности и дополнительного образования (проведение классных часов по вопросам угрозы личной безопасности в сети Интернет, личный профиль в сети Интернет, цифровой след или «Я в сети», приватность и личные границы, мобильное устройство и безопасность в сети Интернет, сетевой этикет; тематические мероприятия - Единый урок по безопасности в сети Интернет, квест по цифровой грамотности «Сетевичок» и др.);

– организации соответствующих мероприятий или обучения в рамках программ воспитания и социализации обучающихся.

Рекомендуется образовательным организациям запланировать курс внеурочной деятельности по информационной безопасности обучающихся. Главная цель курса – обеспечить социальные аспекты информационной безопасности в воспитании культуры информационной безопасности у школьников в условиях цифрового мира, включение на регулярной основе цифровой гигиены в контекст воспитания и обучения детей, формирование личностных и метапредметных результатов воспитания и обучения детей в информационном обществе. Существуют следующие образовательные программы учебного курса «Информационная безопасность»:

–Примерная образовательная программа учебного предмета «Информатика» (модуль «Информационная безопасность») для образовательных организаций, реализующих образовательные программы основного общего образования.

–Примерная образовательная программа учебного курса «Информационная безопасность» для образовательных организаций, реализующих программы основного общего образования (программа курса рассчитана на 30 учебных часов и может быть реализована как за один год обучения, так и непрерывно с 5 по 6 класс / с 7 по 9 класс по модулям содержания).

–Примерная образовательная программа учебного курса «Информационная безопасность» для образовательных организаций, реализующих программы среднего общего образования (программа курса рассчитана на 30 учебных часов и может быть реализована как за один год обучения, так и непрерывно с 1 по 11 класс по модулям содержания).

–Примерная образовательная программа учебного курса «Информационная безопасность» для образовательных организаций, реализующих программы начального общего образования (программа курса рассчитана на 30 учебных часов и может быть

реализована как за один год обучения, так и непрерывно с 1 по 4 класс по модулям содержания).

При преподавании и изучении обучающимися вопросов информационной безопасности рекомендуется не только рассмотреть информационные, потребительские, технические и коммуникативные аспекты информационной безопасности, но и вопросы практического использования сети Интернет для собственного развития и образования.

В работе на занятиях по формированию информационной безопасности детей могут быть использованы следующие ***формы работы***:

– дискуссии или дебаты;

– деловые игры;

– подготовка обучающимися тематических буклетов, листовок и других материалов;

– квесты, премии, конкурсы и олимпиады;

– анкетирование, исследования и опросы;

– тесты и викторины;

– демонстрация мультфильмов и (или) видеоурока;

– семинар, вебинар или занятие с приглашенным экспертом.

При проведении уроков и занятий по информационной безопасности рекомендуется использование технологий неформального обучения - любой организованный и устойчивый процесс коммуникации, порождающий обучение, в котором четко обозначены цели, методы, результаты образовательной деятельности и осуществляемый вне рамок системы традиционного обучения. Одной из технологий организации неформального обучения является кейс-технология.

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

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

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

– текстовые материалы: интервью, фрагмент программы развития, характеристику результатов исследования, статьи и художественные тексты (или их фрагменты), результаты проведенных мониторингов и т. п.;

– иллюстративные материалы: фотографии, диаграммы, таблицы, фильмы, аудиозаписи.

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

При проведении уроков и занятий также рекомендуется использовать игровые методики:

– уроки, напоминающие публичные формы общения: пресс-конференция, брифинг, аукцион, бенефис, регламентированная дискуссия, панорама, телемост, репортаж, диалог, «живая газета», устный журнал и т.д.;

– уроки, основанные на имитации деятельности учреждений и организаций: следствие, органы власти, патентное бюро, ученый совет и т.д.;

– уроки, основанные на имитации деятельности при проведении общественно-культурных мероприятий: заочная экскурсия, экскурсия в прошлое, путешествие, прогулки и т.д.

Рекомендуется после поведения уроков и занятий раздавать обучающимся листовки, содержащие основные аспекты информационной безопасности, которые образовательные организации могут распечатать самостоятельно.

Для подготовки мероприятий по информационной безопасности для обучающихся рекомендуется использовать:

– требования нормативных правовых актов, приведенных в разделе 1;

– теоретические аспекты и информацию, представленные в разделах 2, 3;

– источники, приведенные в приложении А и приложении Б.

Ожидаемые результаты мероприятий по информационной безопасности для обучающихся заключаются в получении знаний и навыков как сделать более безопасным и полезным свое общение в Интернете и иных информационно-телекоммуникационных сетях, а именно:

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

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

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

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

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

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

– анализировать степень достоверности информации и подлинность ее источников;

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

Для обеспечения информационной безопасности обучающихся важным элементом является обеспечение санитарно-эпидемиологических требований при работе с компьютерной техникой как в образовательной организации так и за домашним компьютером.

–По данному вопросу педагогическим работникам рекомендуется ознакомиться и использовать в работе МР 2.4.0330-23 «Гигиена детей и подростков. Методические рекомендации по обеспечению санитарно-эпидемиологических требований при реализации образовательных программ с применением электронного обучения и дистанционных образовательных технологий. Методические рекомендации», утвержденные Главным государственным санитарным врачом РФ 29.08.2023.

–Документ содержит комплекс предложений по созданию условий для внедрения цифровой образовательной среды для детей и молодежи, осваивающих образовательные программы дошкольного, начального общего, основного общего, среднего общего, среднего профессионального и дополнительного образования с применением электронного обучения

и дистанционных образовательных технологий с учетом санитарно-эпидемиологических требований.

– В рекомендациях приводятся, в частности, примеры расположения рабочих мест обучающихся, использующих персональные компьютеры, рекомендуемые формы двигательной активности в режиме учебного дня, рекомендуемые упражнения для физкультурных минуток, а также рекомендации для родителей по сокращению экранного времени у детей.

ПРОСВЕТИТЕЛЬСКИЕ МЕРОПРИЯТИЯ ПО ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ С РОДИТЕЛЯМИ И ЗАКОННЫМИ ПРЕДСТАВИТЕЛЯМИ ОБУЧАЮЩИХСЯ

Обучение детей и подростков по вопросам информационной безопасности не заканчивается в образовательной организации. В данном вопросе должны принимать активное участие родители и законные представители обучающихся.

На сегодняшний день наличие домашнего компьютера или других гаджетов (смартфон, планшет) с выходом в сеть Интернет, к которым у обучающихся есть доступ является нормой, а не привилегией. Естественно, педагогические работники не имеют возможности, да и не должны, отслеживать доступ к какой информации получает обучающийся вне пределов образовательной организации – это прерогатива и прямая обязанность его родителей и законных представителей.

Для обеспечения информационной безопасности детей для родителей (законных представителей) рекомендуется соблюдение ряда правил:

1. Внимательное отношение к действиям своих детей в Интернете - родителям следует активно участвовать в общении ребёнка с Интернетом, особенно на этапе освоения, и не отправлять его в «свободное плавание» по сети. Родители должны обязательно следить за виртуальными контактами детей и знакомиться с сайтами, которые они посещают; интересоваться, кто его друзья в сети так же, как и реальными друзьями.

2. Независимо от возраста ребенка следует использовать программное обеспечение, помогающее фильтровать и контролировать информацию (например, программное обеспечение с функциями «родительского контроля»), но не полагаться полностью на него. Внимание родителя к ребенку - главный метод защиты.

3. Если ребенок имеет аккаунт на одном из социальных сервисов (LiveJournal, blogs.mail.ru, vkontakte.ru и т.п.), следует внимательно изучить, какую информацию помещают его участники в своих профилях и блогах, включая фотографии и видео.

4. Периодические проверки, с какими другими сайтами связан социальный сервис ребенка – его странички могут быть безопасными, но могут и содержать ссылки на нежелательные и опасные сайты (например, порносайт или сайт, на котором друг упоминает номер сотового телефона ребенка или домашний адрес).

5. Постоянное напоминание детям и подросткам о возможностях и опасностях работы с ресурсами Интернет. Родителям необходимо объяснять своему ребёнку, что если он столкнулся с негативом или насилием со стороны другого пользователя, то обязательно должен сообщить об этом близким людям.

6. Следует стимулировать детей сообщать обо всем странном или отталкивающем, а также реагировать, когда они этого не делают (из-за опасения потерять доступ к Интернету дети не говорят родителям о проблемах, а также могут начать использовать Интернет вне дома и школы).

7. Важно контролировать трату денежных средств при скачивании платной информации и получению платных услуг, особенно путём отправки денег. Родителям рекомендуется сформировать список полезных, интересных и безопасных ресурсов, которыми могут пользоваться их дети.

Одно из главных правил для родителей, которым небезразлична информационная безопасность их детей – повышение своего уровня компьютерной грамотности.

Образовательная организация может для повышения уровня знаний родителей и законных представителей обучающихся в вопросах обеспечения информационной безопасности детей предпринимать различные регулярные меры информационного и организационного характера, в частности:

1. Освещение вопросов информационной безопасности детей в рамках проводимых родительских собраний и проведение тематических собраний для родителей с участием педагогических работников и представителей администрации образовательной организации, в частности для демонстрации видеоматериалов по данным вопросам.

2. Организация индивидуальных и групповых консультаций родителей и законных представителей обучающихся классными руководителями, специалистами психологической службы и администрации образовательной организации для обеспокоенных родителей и законных представителей обучающихся и родителей и законных представителей обучающихся, находящихся в группе риска.

3. Проведение семинаров, лекций и вебинаров с участием экспертов и сотрудников правоохранительных органов для родителей и законных представителей обучающихся.

4. Раздача информационных материалов об обеспечении безопасности детей в сети Интернет, в частности памятки, флаеры и другие материалы.

5. Проведение анкетирования родителей и законных представителей обучающихся по вопросам организации дома мер по обеспечению защиты детей в информационном пространстве.

6. Размещение на сайте образовательной организации, средствах массовой информации образовательной организации, сообществах в социальной сети и сервисе электронных дневников для родителей и законных представителей обучающихся информации по обеспечению информационной безопасности детей.

В ходе мероприятий для родителей и законных представителей обучающихся рекомендуется выделить следующие темы:

– важность обеспечения цифровой и информационной грамотности детей и подростков;

– рекомендации и советы по обеспечению информационной безопасности личности и детей как особо незащищенных пользователей сети Интернет;

– методы и функции родительского контроля.

Вопросы информационной безопасности детей для родителей или законных представителей детей имеют свою специфику, отражающую необходимые им знания для обеспечения защиты детей в информационном пространстве с учетом специфики каждого возраста.

Общие советы родителям и законным представителям по безопасности в сети Интернет для детей возраста 7-12 лет:

1. Создайте список домашних правил посещения Интернета при участии детей и требуйте его выполнения.

2. Требуйте от вашего ребенка соблюдения временных норм нахождения за компьютером. Покажите ребенку, что вы наблюдаете за ним не потому что вам это хочется, а потому что вы беспокоитесь о его безопасности и всегда готовы ему помочь.

3. Компьютер с подключением к Интернету должен находиться в общей комнате под присмотром родителей.

4. Используйте средства блокирования нежелательного контента как дополнение к стандартному родительскому контролю.

5. Создайте семейный электронный ящик, чтобы не позволить детям иметь собственные адреса, а для старшего возраста настаивайте на том, чтобы дети предоставляли вам доступ к своей электронной почте, чтобы вы убедились, что они не общаются с незнакомцами.

6. Приучите детей советоваться с вами перед опубликованием какой-либо информации средствами электронной почты, чатов, регистрационных форм и профилей.

7. Приучите детей никогда не выдавать личную информацию средствами электронной почты, чатов, систем мгновенного обмена сообщениями, регистрационных форм, личных профилей и при регистрации на конкурсы в Интернете.

8. Научите детей не загружать файлы, программы или музыку без вашего согласия.

9. Приучите детей не загружать программы без вашего разрешения. Объясните им, что они могут случайно загрузить вирусы или другое нежелательное программное обеспечение.

10. В «белый» список сайтов, разрешенных для посещения, вносите только сайты с хорошей репутацией.

11. Не забывайте беседовать с детьми об их друзьях в Интернете, как если бы речь шла о друзьях в реальной жизни.

12. Не делайте «табу» из вопросов половой жизни, так как в Интернете дети могут легко наткнуться на порнографию или сайты "для взрослых".

13. Настаивайте, чтобы дети никогда не соглашались на личные встречи с друзьями по Интернету.

14. Объясните детям, что нельзя использовать сеть для хулиганства, распространения сплетен или угроз.

15. Приучите вашего ребенка сообщать вам о любых угрозах или тревогах, связанных с Интернетом. Оставайтесь спокойными и напомните детям, что они в безопасности, если сами рассказали вам о своих тревогах. Похвалите их и посоветуйте подойти еще раз в подобных случаях.

Советы родителям и законным представителям по безопасности в сети Интернет для подростков от 13 до 17 лет.

В этом возрасте подростки активно используют поисковые сайты, электронную почту, службы мгновенного обмена сообщениями, скачивают музыку и фильмы. Зачастую в данном возрасте родителям уже сложно контролировать своих детей, которые об Интернете уже знают значительно больше них.

Тем не менее, важно по-прежнему строго соблюдать правила Интернет-безопасности - соглашение между родителями и детьми. В дополнение к списку, приведенному ранее, обратите внимание:

1. Обговорите список запрещенных сайтов («черный список»), часы работы в Интернете, руководство по общению в Интернете (в том числе в чатах).

2. Не забывайте беседовать с детьми об их друзьях в Интернете, о том, чем они заняты таким образом, будто речь идет о друзьях в реальной жизни. Спрашивайте о людях, с которыми дети общаются посредством служб мгновенного обмена сообщениями, чтобы убедиться, что эти люди им знакомы.

3. Научите подростков не выдавать в Интернете своего реального электронного адреса, не отвечать на нежелательные письма и использовать специальные почтовые фильтры.

4. Приучите себя знакомиться с сайтами, которые посещают подростки.

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

6. Обсудите с подростками проблемы сетевых азартных игр и их возможный риск. Напомните, что дети не могут играть в эти игры согласно закону.

Кроме того, необходимо как можно чаще просматривать отчеты о деятельности детей в Интернете. Это не нарушение личного пространства несовершеннолетнего, а мера предосторожности и проявление родительской ответственности и заботы.

Приложение А
к методическим рекомендациям

МЕТОДИЧЕСКИЕ МАТЕРИАЛЫ ДЛЯ ОРГАНИЗАЦИИ ПОДГОТОВКИ ПЕДАГОГОВ К ПРОВЕДЕНИЮ ПРОСВЕТИТЕЛЬСКИХ МЕРОПРИЯТИЙ ПО ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

Название методического материала	Адрес в сети Интернет	Рекомендации по использованию
Методические рекомендации по основам информационной безопасности для обучающихся общеобразовательных организаций с учётом информационных, потребительских, технических и коммуникативных аспектов информационной безопасности	https://ulgimnaz34.gosuslugi.ru/netcat_files/30/69/1567575522_metodich.rekomendacii_po_osnovam_informacionnoy_bezopasnosti_dlya_obuchayushihsya.pdf?ysclid=lspung7mkk177266008	Разработаны в соответствии с пунктом 8 приказа Минкомсвязи России от 27.02.2018 года № 88 «Об утверждении плана мероприятий по реализации Концепции информационной безопасности детей на 2018-2020 годы». Методические рекомендации направлены на организацию преподавания основ информационной безопасности в общеобразовательных организациях РФ.
Методические рекомендации для несовершеннолетних, родителей (законных представителей) несовершеннолетних, наглядные информационные материалы по безопасному использованию сети «Интернет» в целях предотвращения преступлений, совершаемых с ее использованием, как самими несовершеннолетними, так и в отношении них	https://tlsvu.mil.ru/upload/site126/document_file/Metodicheskie_rekomendacii_Minprosvescheniya_Rossii_ot_29.12.2021__bn_Internet_i_deti.pdf?ysclid=lspun67ox2496801964	Методические рекомендации Министерство просвещения РФ, ФГБУ «Центр защиты прав и интересов детей». Подготовлены в рамках выполнения работ по организации проведения общественно-значимых мероприятий в сфере образования, науки и молодежной политики в целях организационно-методического сопровождения развития системы профилактики девиантного поведения несовершеннолетних в части организационно-методического сопровождения реализации Концепции развития системы профилактики безнадзорности и правонарушений несовершеннолетних в субъектах РФ.
Методические рекомендации по вопросам информационной безопасности детей в сети Интернет. Составители: Шарипова Г.И., Тагиров И.Х. Уфа, 2018	https://gbpoudmk.ru/wp-content/uploads/2018/09/Методические-рекомендации-по-вопросам-информационной-безопасности-детей-в-сети-Интернет.pdf	Цель методических рекомендаций - помочь педагогам, родителям и обучающимся усвоить правила пользования Интернетом, знать источники опасности, которые таит в себе всемирная паутина, и первоочередные шаги для обеспечения безопасности

Название методического материала	Адрес в сети Интернет	Рекомендации по использованию
Информационная безопасность несовершеннолетних. (методические рекомендации для проведения занятий с обучающимися)	https://shkolagreczovskaya-r71.gosweb.gosuslugi.ru/netcat_files/30/69/metodicheskie_rekomendatsii_inf_bezopasnost_.pdf	Представлены общие рекомендации по проведению мероприятий по информационной безопасности: – урок «Интернет-безопасность» (1-11 классы); – анкетирование обучающихся; – круглый стол «Основы безопасности в сети Интернет»; – компьютерная игра для младших школьников; – флэш-мобы по проблемам информационной безопасности
Курс «Основы кибербезопасности» Составители: Тонких И.М., Комаров М.М., Ледовской В.И., Михайлов А.В. Москва, 2016	https://toipkro.ru/content/files/documents/podrazdeleniya/ordo/ciber%20bezopasnost.pdf?ysclid=lspv0zx75v893188205	Методический материал представляет собой межпредметный курс, посвященный актуальным вопросам обеспечения безопасности в сети Интернет (техника безопасности и эргономика, сетевой этикет, мошеннические действия в сети Интернет, правовые основы кибербезопасности и т.д.). Методический материал содержит примеры разработок уроков, посвященных способам защиты от угроз сети Интернет. Представленные материалы будут полезны педагогам при проектировании содержания программ внеурочной деятельности, уроков информационной безопасности
Основы кибербезопасности. 5-11 класс. Учебно-методическое пособие. Автор: Вангородский С.Н.	https://rosuchebnik.ru/material/osnovy-kiberbezopasnosti-5-11-klass-uchebno-metodicheskoe-posobie/	Пособие адресовано учителям и учащимся общеобразовательных организаций, а также родителям школьников. В нем представлены наиболее распространенные виды киберугроз, цели и задачи системы кибербезопасности, небезопасные для детей и подростков интернет-сервисы. Для педагогов и родителей в пособии предлагается полезная информация о программах контроля, позволяющих защитить школьников от опасных сайтов, и методические рекомендации по формированию у детей и подростков навыков безопасного поведения в Интернете.

Название методического материала	Адрес в сети Интернет	Рекомендации по использованию
Безопасный Интернет детям	https://мвд.рф/безопасный-интернет-детям	Урок, посвященный проблемам кибербезопасности, проведенный сотрудниками МВД России в одной из школ г. Москва, давший старт всероссийской профилактической акции для детей «Безопасный Интернет детям». Дополнительно представлено типовой сценарий урока «Безопасный Интернет детям»
Угрозы детской кибербезопасности. Методическое пособие для педагогов Вологда, 2022	https://milytin.ru/attachments/article/438/Методическое%20пособие.%20Угрозы%20детской%20кибербезопасности.pdf?ysclid=lspverocog162986236	В пособии представлено нормативно-правовое обеспечение, приоритетные задачи государственной политики в области информационной безопасности детей, угрозы сети Интернет для детей, рекомендации по обеспечению безопасности…
Онлайн-курс “Безопасность в Интернете” от Академии Яндекса	https://stepik.org/course/191/promo	Онлайн-курс содержит информацию о видах мошенничества в сети Интернет и о том, как им противостоять. Курс рассчитан на обучающихся 6-9 классов, но он будет полезен родителям, педагогам, планирующим проведение урока по безопасности в сети Интернет. Материалы курса будут полезны при подготовке практикумов, обеспечения поддержки реализации программ внеурочной деятельности. Материалы курса имеют бесплатный доступ
Методическое пособие “Медиаграмотность. Как жить в медиамире” Автор Дубовер Д. Ростов-на-Дону, 2015	https://biuv-school9tihvin.eduface.ru/uploads/24300/24236/section/451751/DOT/Metodicheskoe_posobie_Mediagramotnost_.pdf	Методическое пособие рассказывает о безопасном поведении ребенка в социальной сети, новостной грамотности, о безопасной работе с почтовым сервисом и облачным хранилищем, об использовании электронных денег и организации родительского контроля. Пособие может быть использовано педагогами при планировании содержания программы внеурочной деятельности, уроков безопасности, классных часов, тематических родительских собраний. Пособие может быть рекомендовано обучающимся и родителям (законным представителям)

Название методического материала	Адрес в сети Интернет	Рекомендации по использованию
Методическое руководство “Полезный и безопасный Интернет. Правила безопасного использования интернета для детей младшего школьного возраста” Автор Солдатова Г. У. Москва, 2012 г.	https://edu.ruobr.ru/media/uploads/documents/bezopasnyi_internet.pdf?ysclid=lspvrc5nbr379492245	Методическая разработка адресована психологам, педагогам начальных классов, классным руководителям, родителям школьников младших классов, представляет собой методическое руководство по планированию занятий с обучающимися начальной школы, посвященных вопросам безопасного пребывания в сети Интернет. Пособие может использоваться педагогами при проработке содержания программы внеурочной деятельности, отдельных занятий и уроков.
Полезный и безопасный интернет. Правила безопасного использования интернета для детей младшего школьного возраста: практическое пособие Под ред. Г.У. Солдатовой Москва, 2017	https://dom-tvorchestva.ru/wp-content/uploads/2022/04/pravila-bezopasnosti-ispolzovaniya-interneta-dlya-detey-mladshego-shkolyn-vozrasta.pdf	Практическое пособие разработано на основе результатов исследований особенностей использования интернета российскими детьми и подростками, осуществленных сотрудниками факультета психологии МГУ имени М.В. Ломоносова и Фонда Развития Интернет в 2009–2016 гг. Практическое пособие адресовано работникам системы образования, психологам, педагогам начальных классов, классным руководителям, педагогам-библиотекарям, преподавателям по информатике и ОБЖ, студентам педагогических и психологических факультетов вузов, родителям школьников младших классов.
Учебно-методическое пособие “Практическая психология безопасности: управление персональными данными в Интернете” Авторы: Солдатова Г.У., Приезжева А.А., Олькина О.И., Шляпников В.Н. Москва, 2017	https://shkola11staryjoskol-r31.gosweb.gosuslugi.ru/netcat_files/30/69/Uchebno_metodicheskoe_posobie_Prakticheskaya_psihologiya_bezopasnosti_upravlenie_personal_nymi_dannymi_v_Internete.pdf	Учебно-методическое пособие посвящено решению задачи повышения цифровой компетентности обучающихся, педагогов, родителей в сфере управления персональными данными в сети Интернет. Включает в себя разработки уроков для педагогов, практикум для обучающихся 6–10-х классов. Материалы к урокам подготовлены с учетом действующего законодательства РФ, а также мирового опыта управления персональными данными в интернете. Материалы пособия могут быть использованы педагогами при планировании содержания программы внеурочной деятельности, планировании уроков безопасности, классных часов, тематических родительских собраний

Название методического материала	Адрес в сети Интернет	Рекомендации по использованию
Дидактическая игра #БУДЬСМЕЛЫМ	Инструкция: https://suurimjulgus.ee/assets/files/Telia_juhis_RU_315x280.pdf Материалы для организации игры: https://suurimjulgus.ee/assets/files/Telia_kaardid_RUS_A4_print.pdf	Дидактическая игра #БУДЬСМЕЛЫМ представляет собой набор кейсов, связанных с разными угрозами сети Интернет. В каждой ситуации обучающиеся должны синтезировать решения проблемы, с которой столкнулся персонаж кейса. Дидактическая игра может использоваться педагогами при проведении уроков безопасности, занятий внеурочной деятельности, уроков информатики, посвященных безопасности в сети Интернет
Интернет-безопасность детей: Методические рекомендации	https://nro.center/wp-content/uploads/2019/10/rekomendacii.pdf	Разработаны в рамках проекта «Безопасная интернет-среда — детям». Материалы отобраны для помощи в обучении подростков безопасному использованию Интернета и повышения их цифровой грамотности.
Методические рекомендации для родителей (законных представителей) о возможностях организации родительского контроля за доступом детей в сеть Интернет	https://liczejgumanitarnyjizhevsk-r18.gosweb.gosuslugi.ru/netcat_files/30/69/recomendacii_internet.pdf?1676012883	Цель данных методических рекомендаций - ознакомить родителей (законных представителей) с возможностью и необходимостью организации родительского контроля за доступом детей в сеть Интернет. Обеспечение безопасности детей в сети Интернет невозможно без привлечения родителей. Часто родители не понимают и недооценивают угрозы, которым подвергается их ребенок, находясь в сети Интернет.
Уроки кибербезопасности в школе (Киберуроки). Сборник методических разработок Пермь, 2022	https://цпмсс.рф/files/biblioteka/КИБЕРУРОКИ_2022_Методические_разработки.pdf	Методические разработки адресованы администрации общеобразовательных учреждений, специалистам, педагогам, классным руководителям для проведения уроков, классных часов по вопросам кибербезопасности. Методические разработки уроков представлены для учащихся в каждой возрастной категории, в том числе для детей с ограниченными возможностями здоровья.

Название методического материала	Адрес в сети Интернет	Рекомендации по использованию
Информационная безопасность. 2–11 классы: методическое пособие для учителя Автор: Цветкова, М.С. Москва, 2020	https://lbz.ru/metodist/authors/ib/ib-mp-tsvetkova.pdf?ysclid=lsiyap2eyv577832717	Методическое пособие представляет примерную программу по учебным курсам информационной безопасности, разработанным на основе учебных пособий в серии «Информационная безопасность» для 2–4, 5–6, 7–9 и 10–11 классов. Для учителей, методистов и преподавателей профессионального образования.

Приложение Б
к методическим рекомендациям

РЕСУРСЫ СЕТИ ИНТЕРНЕТ ДЛЯ ИСПОЛЬЗОВАНИЯ В РАБОТЕ ПО ОБЕСПЕЧЕНИЮ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ ОБУЧАЮЩИХСЯ В СЕТИ ИНТЕРНЕТ

Название ресурса	Адрес в сети Интернет	Краткая аннотация	Рекомендации по использованию
Единый урок безопасности в сети Интернет	https://www.единыйурок.рф/?ysclid=lspw8xn5io333930670	Портал Единыйурок.рф - онлайн-площадка для проведения Единых уроков, тематических занятий и образовательных мероприятий, рекомендованных МОиН РФ.	Педагогические работники образовательных организаций найдут на сайте рекомендации по проведению единого урока безопасности в сети Интернет, разработке программ внеурочной деятельности по данной теме, могут пройти дистанционные курсы повышения квалификации “Основы кибербезопасности”, “Информационная компетентность педагога”. Руководящие работники образовательных организаций могут использовать материалы портала при планировании мероприятий общешкольного характера, при оформлении информационных стендов, при проведении родительских собраний, обучающих семинаров для педагогов
Официальный портал МВД России “Безопасный Интернет-детям”	https://мвд.рф/mvd/structure1/Upravlenija/убк/безопасный-интернет-детям?ysclid=lspwb5rvll504694675	Раздел официального сайта МВД России содержит памятки по обеспечению информационной безопасности детей и молодежи в сети Интернет, тесты на знание правил поведения в сети Интернет	Материалы будут полезны педагогам при организации единых уроков безопасности в сети Интернет, проведении классных часов, оформлении информационных стендов, проведении тематических родительских собраний

Название ресурса	Адрес в сети Интернет	Краткая аннотация	Рекомендации по использованию
Портал “Сетевичок”	https://сетевичок.рф/?ysclid=lspwfdyi9k295373352	Информационный портал для обеспечения информационной поддержки международного квеста по цифровой грамотности #СЕТЕВИЧОК, конкурса детских и молодежных сайтов #ПРЕМИЯСЕТЕВИЧОК	Материалы, представленные на портале, могут использоваться учителями информатики при проведении уроков информатики или занятий внеурочной деятельности, посвященных сайтостроению. Конкурс #ПРЕМИЯСЕТЕВИЧОК будет уместно рекомендовать обучающимся как источник информации по обеспечению безопасности персонального сайта.
Лига безопасного интернета	https://ligainternet.ru/?ysclid=lspwdtyql193308932	Лига безопасного Интернета - учреждена в 2011 году при поддержке МВД России, Минкомсвязи и Комитета Государственной Думы по вопросам семьи, женщин и детей. Основная цель - создание безопасного пространства Интернета на территории РФ.	Ключевые направления деятельности: – проведение уроков «Безопасного Интернета» в общеобразовательных учреждениях и ВУЗах; – оказание методической помощи педагогам и преподавателям школ; – подготовка методических материалов и учебных пособий по безопасности в сети Интернет и др.
Защита детей от вредной информации в сети интернет (Сайт для умных родителей)	http://www.internet-kontrol.ru/?ysclid=lspwjliarv458739194	Информационный ресурс для родителей. Собрана подборка статей о защите детей в Интернете, рассказывается о всевозможных поисковых сервисах, созданных специально для детей, о том, как обеспечить защиту детей с помощью настроек операционной системы, какие бывают программы для защиты детей в Интернет	Подборка статей, размещенных на информационном портале, может быть рекомендована родителям обучающихся в качестве источника информации об угрозах сети Интернет, способах защиты от угроз сети Интернет. Материалы могут быть рекомендованы педагогами обучающимся.

Название ресурса	Адрес в сети Интернет	Краткая аннотация	Рекомендации по использованию
Министерство юстиции РФ. Федеральный список экстремистских материалов	https://minjust.gov.ru/ru/extremist-materials/	Раздел официального сайта Министерства юстиций РФ содержит перечень материалов экстремистского характера, запрещенных к использованию	Материалы портала могут использоваться при проектировании элементов содержания программ повышения квалификации для руководящих работников образовательных организаций, при проведении лекционных занятий, посвященных проблеме организации контентной фильтрации. Ресурс может быть использован руководящими работниками образовательных организаций при организации системы контентной фильтрации
Реестр запрещенных сайтов	https://eais.rkn.gov.ru https://www.rubanlist.com https://reestr.rublacklist.net/ru/?ysclid=lspwok694v255744248	Информационный ресурс содержит перечень запрещенных в РФ сайтов и ресурсов. Сайт предназначен исключительно для мониторинга Реестра запрещенных сайтов, не является каталогом	Материалы портала могут использоваться при проектировании элементов содержания программ повышения квалификации для руководящих работников образовательных организаций, при проведении лекционных занятий, посвященных проблеме организации контентной фильтрации. Ресурс может быть использован руководящими работниками образовательных организаций при организации системы контентной фильтрации
Азбука цифрового мира.	https://www.edu.yar.ru/azbuka/?ysclid=lspwpovryx989623424	На сайте размещены увлекательные комиксы, специализированные тренажёры и интересные игры	Материалы сайта будут полезны педагогам при проработке содержания программы внеурочной деятельности, уроков безопасности в сети Интернет, классных часов, занятий внеурочной деятельности. Комиксы и тренажеры могут быть рекомендованы обучающимся как общеразвивающий безопасный контент сети Интернет

Название ресурса	Адрес в сети Интернет	Краткая аннотация	Рекомендации по использованию
Персональные данные. Дети.	https://персональныеданные.дети/?ysclid=lspwr9ib48453872043	Портал проекта Роскомнадзора содержит базу материалов в виде правил, памяток, презентаций, тестов и игр по актуальным вопросам безопасности персональных данных обучающихся в сети Интернет.	Материал знакомит обучающихся 6-11 класса с понятием персональные данные, правилами конфиденциальности в сети Интернет. Среди представленных материалов размещены инструкции для родителей (законных представителей), педагогов.