

ПРАВИТЕЛЬСТВО РОССИЙСКОЙ ФЕДЕРАЦИИ

РАСПОРЯЖЕНИЕ от 2 декабря 2015 г. N 2471-р

1. Утвердить прилагаемую Концепцию информационной безопасности детей (далее - Концепция).
2. Минкомсвязи России совместно с другими заинтересованными федеральными органами исполнительной власти обеспечить реализацию Концепции.
3. Рекомендовать органам исполнительной власти субъектов Российской Федерации при формировании и осуществлении региональных программ в сфере информационной безопасности детей учитывать положения Концепции.
4. Реализация Концепции осуществляется заинтересованными федеральными органами исполнительной власти в пределах бюджетных ассигнований, предусмотренных им в федеральном бюджете на соответствующий финансовый год.

*Председатель Правительства
Российской Федерации
Д. МЕДВЕДЕВ*

*УТВЕРЖДЕНА
распоряжением Правительства
Российской Федерации
от 2 декабря 2015 г. N 2471-р*

КОНЦЕПЦИЯ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ ДЕТЕЙ

I. Общие положения

Стремительное развитие информационных технологий заставило современное поколение детей и подростков (далее - дети) столкнуться с принципиально новыми вызовами. Взросление, обучение и социализация детей проходят в условиях гиперинформационного общества.

Процесс социализации через традиционные институты (семьи, школы) все активнее дополняется средствами массовой информации и массовых коммуникаций, особенно информационно-телекоммуникационной сетью "Интернет" (далее - сеть "Интернет"), которые становятся важнейшими институтами социализации, образования и просвещения нового поколения, в определенной мере замещая традиционно сложившиеся формы. Главным образом это происходит в тех случаях, когда родители (законные представители) в семье отстраняются от своих обязанностей по воспитанию и развитию детей и перекладывают их на внешних игроков.

При разумном и эффективном сотрудничестве общественных и государственных институтов информационные и коммуникационные технологии могут быть ключевыми элементами политики, способствующими сохранению

культуры России, укреплению нравственных и патриотических принципов в общественном сознании, а также развитию системы культурного и гуманитарного просвещения.

II. Основные принципы обеспечения информационной безопасности детей

Исходя из понимания информационной безопасности детей как защиты ребенка от дестабилизирующего воздействия информационной продукции и создания условий информационной среды для позитивной социализации и индивидуализации, оптимального социального, личностного, познавательного и физического развития, сохранения психического и психологического здоровья и благополучия, а также формирования позитивного мировосприятия, государственная политика в области обеспечения информационной безопасности детей основывается на конституционных гарантиях равенства прав и свобод граждан и реализуется в соответствии со следующими принципами:

признание детей равноправными участниками процесса формирования информационного общества в Российской Федерации;

ответственность государства за соблюдение законных интересов детей в информационной сфере;

необходимость формирования у детей умения ориентироваться в современной информационной среде;

воспитание у детей навыков самостоятельного и критического мышления;

развитие государственно-частного партнерства в целях обеспечения законных интересов детей в информационной среде;

повышение эффективности сотрудничества представителей средств массовой информации и массовых коммуникаций и государственных органов в интересах защиты детей от информации, способной причинить вред их здоровью и развитию;

обучение детей медиаграмотности;

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

создание условий для формирования в информационной среде благоприятной атмосферы для детей вне зависимости от их социального положения, религиозной и этнической принадлежности;

взаимодействие различных ведомств при реализации стратегий и программ в части, касающейся обеспечения информационной безопасности детей;

обеспечение широкого доступа детей к историческому и культурному наследию России через использование современных средств массовых коммуникаций;

открытость и взаимодействие с другой информационной культурой и традициями, формирование у детей объективного представления о российской культуре как неотъемлемой части мировой цивилизации.

III. Приоритетные задачи государственной политики в области информационной безопасности детей

Стратегической целью государственной политики в области информационной безопасности детей является обеспечение гармоничного развития молодого поколения при условии минимизации всех негативных факторов, связанных с формированием гиперинформационного общества в России.

Обеспечение информационной безопасности детей возможно исключительно при условии эффективного сочетания государственных и общественных усилий при определяющей роли семьи.

В связи с этим важнейшей задачей является налаживание согласованного взаимодействия семьи, главного института социализации и воспитания детей, с государством и всеми элементами современного медиарынка - производителями и распространителями контента, психолого-педагогическими экспертными сообществами и экспертными сообществами в области художественного образования. Только тесное сотрудничество всех участников медиаиндустрии позволит построить эффективную систему регулирования потребления информационной продукции, максимально безопасную для психического и физического развития и здоровья подрастающего поколения.

Семья, государство и заинтересованные в обеспечении информационной безопасности детей общественные организации имеют следующие приоритетные задачи:

формирование у детей навыков самостоятельного и ответственного потребления информационной продукции;

повышение уровня медиаграмотности детей;

формирование у детей позитивной картины мира и адекватных базисных представлений об окружающем мире и человеке;

ценностное, моральное и нравственно-этическое развитие детей;

воспитание у детей ответственности за свою жизнь, здоровье и судьбу, изживание социального потребительства и инфантилизма;

усвоение детьми системы семейных ценностей и представлений о семье;

развитие системы социальных и межличностных отношений и общения детей;

удовлетворение и развитие познавательных потребностей и интересов ребенка, детской любознательности и исследовательской активности;

развитие творческих способностей детей; воспитание у детей толерантности;

развитие у детей идентичности (гражданской, этнической и гендерной);

формирование здоровых представлений о сексуальной жизни человека;

эмоционально-личностное развитие детей;

формирование у детей чувства ответственности за свои действия в информационном пространстве;

воспитание детей как независимых, ответственных и самостоятельно мыслящих личностей с целью изживания социального иждивенчества.

Кроме того, совместные усилия всех участников медиарынка должны быть направлены на минимизацию рисков десоциализации, развития и закрепления девиантного и противоправного поведения детей, включая такие недопустимые формы поведения, как:

агрессивное поведение, применение насилия и проявление жестокости по отношению к людям и животным;

совершение действий, представляющих угрозу жизни и (или) здоровью ребенка, в том числе причинение вреда своему здоровью, суицид;

употребление наркотических средств, психотропных и (или) одурманивающих веществ, табачных изделий, алкогольной и спиртосодержащей продукции, пива и напитков, изготавливаемых на их основе;

занятие проституцией; бродяжничество; попрошайничество;

иные виды противоправного поведения и (или) преступлений.

IV. Механизмы реализации государственной политики в области информационной безопасности детей

Анализ международного опыта показывает, что в мировой практике присутствуют три возможных варианта регулирования информационного потребления с целью обеспечения безопасности детей: государственное регулирование, саморегулирование медиа и сорегулирование медиа и государства. В каждой стране сделан выбор в пользу одного из трех вариантов. Третий вариант имеет значительные преимущества перед первыми двумя вариантами, представляется наиболее эффективным и позволяет добиться желаемого успеха, если учитывает психолого-педагогические и художественно-культурные характеристики информационной продукции.

Учет психолого-педагогического и художественно-культурного аспектов при оценке содержания информационной продукции в контексте обеспечения информационной безопасности детей позволяет обеспечить личностное, морально-нравственное и культурное развитие детей - участников глобального информационного процесса.

Возрастно-психологический подход к оценке вредного воздействия информационной продукции на психическое развитие, здоровье и психологическое благополучие детей, который лег в основу Федерального [закона](#) "О защите детей от информации, причиняющей вред их здоровью и развитию", показал свою достаточно высокую эффективность.

Вместе с тем при возрастной маркировке информационной продукции необходимо учитывать, что ее основной задачей является не развернутая характеристика информационного продукта, а сигнализирование родителям о том, что он содержит информацию, которая может представлять угрозу для ребенка. Кроме того, нецелесообразно расширенное толкование правоприменителями таких терминов, как "насилие и жестокость", которое может привести к тому, что дети будут ограничены в доступе к информационной продукции военно-исторической направленности, являющейся в условиях современного общества важнейшим элементом формирования патриотических убеждений у молодого поколения.

Однако для обеспечения информационной безопасности детей наряду с запретом информационной продукции, которая может причинить вред развитию и здоровью ребенка, государству и обществу необходимо содействовать созданию условий, обеспечивающих позитивную социализацию и индивидуализацию ребенка, его психологическое благополучие и позитивное мировосприятие.

Необходима также организация последовательных и регулярных мероприятий государства и общественных организаций, направленных на повышение уровня медиаграмотности детей, которые должны с раннего возраста приобретать навыки безопасного существования в современном информационном пространстве. Стремительное развитие информационных и коммуникационных ресурсов, возрастающая доступность медиасредств (в первую очередь смартфонов и планшетных компьютеров) открывают перед детьми практически безграничные возможности для доступа к информации самого разного свойства, в том числе и к такой, которая может нанести вред их психическому и нравственному развитию. Усилия государства по ограничению доступа к ресурсам,

содержащим противоправный контент, не смогут полностью оградить детей от вредной информации. Поэтому необходимо формировать у детей механизмы критической оценки получаемых сведений. Совместные усилия семьи, общественных организаций и государства должны быть направлены на выработку у детей навыка самостоятельной оценки контента, умения анализировать и отличать настоящие новости от дезинформации, противостоять манипулированию и зловредной рекламе асоциального поведения.

Кроме того, необходимо продолжение активной деятельности контролирующих и правоохранительных органов по пресечению фактов незаконного распространения на территории страны печатной и аудиовизуальной продукции, запрещенной к обороту законодательством Российской Федерации, в том числе пропагандирующей культ насилия и жестокости, порнографию, экстремистскую деятельность, потребление наркотических средств и психотропных веществ, а также информационной продукции, запрещенной или ограниченной для реализации несовершеннолетним. Важным элементом этого процесса может быть привлечение журналистских сообществ, организаций саморегулирования и общественных организаций.

Необходимо продолжать работу по совершенствованию механизма блокировки сайтов в сети "Интернет", содержащих запрещенную информацию. В настоящий момент доказала свою высокую эффективность существующая система включения (по решению уполномоченных Правительством Российской Федерации федеральных органов исполнительной власти) пяти видов особо социально опасной информации, доступ к которой безусловно должен быть запрещен, в Единый реестр доменных имен, указателей страниц сайтов в сети "Интернет" и сетевых адресов, позволяющих идентифицировать сайты в сети "Интернет", содержащие информацию, распространение которой в Российской Федерации запрещено. К таким видам информации относится детская порнография, информация о продаже и изготовлении наркотиков, призывы к осуществлению самоубийств, информация о несовершеннолетнем, пострадавшем в результате противоправных действий (бездействия), информация, нарушающая требования Федерального [закона](#) "О государственном регулировании деятельности по организации и проведению азартных игр и о внесении изменений в некоторые законодательные акты Российской Федерации" и Федерального [закона](#) "О лотереях" о запрете деятельности по организации и проведению азартных игр и лотерей с использованием сети "Интернет" и иных средств связи.

Процесс перехода Российской Федерации к постиндустриальному обществу сопровождается последовательной компьютеризацией общеобразовательных организаций и организаций дополнительного образования, иных учреждений для несовершеннолетних, включая детские и юношеские библиотеки. В связи с этим целесообразно предусмотреть внедрение эффективных современных технических и программных средств защиты детей от информации, причиняющей вред их здоровью, нравственному и духовному развитию, обеспечение соблюдения установленных правил гигиены и безопасности при пользовании компьютерной техникой. Для этого необходимо формирование механизма эффективного использования средств, выделяемых из федерального бюджета и бюджетов субъектов Российской Федерации на компьютеризацию школ и детских библиотек. Вместе с этим необходимо обеспечить в детских и юношеских библиотеках (с сохранением осуществляемых ими в настоящее время функций) медиабезопасность детей, создавая для этого соответствующие технические и организационные условия, а также правовые механизмы.

Кроме того, государству следует поддерживать создание и осуществление деятельности организаций саморегулирования средств массовой информации и массовых коммуникаций, а также общественных движений и объединений, ассоциаций и движений родительской общественности, ассоциаций потребителей продукции средств массовой информации, образовательных и телекоммуникационных услуг, осуществляющих функции наблюдения (мониторинга) и общественного контроля за соблюдением законодательства Российской Федерации о средствах массовой информации и о рекламе. Перспективными являются также разработка и внедрение специальных образовательных и просветительских программ, содержащих информацию об информационных угрозах, о правилах безопасного пользования детьми сетью "Интернет", средствах защиты несовершеннолетних от доступа к информации, наносящей вред их здоровью, нравственному и духовному развитию, предназначенных для родителей, работников системы образования, детских и юношеских библиотек и других специалистов, занятых обучением и воспитанием несовершеннолетних, организацией их досуга.

Следует также продолжать широкомасштабные государственные и общественные эмпирические исследования с целью оценки эффективности политики по защите детей от негативной информации.

Усилия семьи, общества и государства должны быть направлены на то, чтобы ребенок с детства привыкал свободно ориентироваться в медиапространстве, умел взаимодействовать с различными источниками информации, не поддавался манипуляциям извне и мог делать самостоятельные выводы о качестве информационных продуктов.

V. Ожидаемые результаты

Реализация Концепции обеспечит в 2020 году формирование в Российской Федерации поколения молодых граждан, которые смогут свободно и самостоятельно ориентироваться в современном информационном пространстве. Будет создана новая медиасреда, соответствующая следующим характеристикам:

наличие развитых информационно-коммуникационных механизмов, направленных на социализацию молодого поколения и раскрытие его творческого потенциала;

свободный доступ детей к историко-культурному наследию предшествующих поколений;

качественный рост уровня медиаграмотности детей; увеличение числа детей, разделяющих ценности патриотизма; гармонизация меж- и внутрипоколенческих отношений; популяризация здорового образа жизни среди молодого поколения; формирование среди детей устойчивого спроса на получение высококачественных информационных продуктов;

снижение уровня противоправного и преступного поведения среди детей;

формирование у детей уважительного отношения к интеллектуальной собственности и авторскому праву, сознательный отказ от использования "пиратского" контента.

**МИНИСТЕРСТВО ПРОСВЕЩЕНИЯ РОССИЙСКОЙ
ФЕДЕРАЦИИ**

**ДЕПАРТАМЕНТ ГОСУДАРСТВЕННОЙ ПОЛИТИКИ В СФЕРЕ
ОБЩЕГО ОБРАЗОВАНИЯ**

ПИСЬМО

от 29 марта 2019 г. N 03-393

О МЕТОДИЧЕСКИХ РЕКОМЕНДАЦИЯХ

Минпросвещения России направляет для учета в работе Методические рекомендации по реализации мер, направленных на обеспечение безопасности детей в сети "Интернет" (далее - Рекомендации), подготовленные Временной комиссией Совета Федерации по развитию информационного общества совместно с МВД России, Минкомсвязи России, Минпросвещения России, Роскомнадзором, Минздравом России и Роспотребнадзором.

Рекомендации представляют собой перечень рекомендаций о различных мерах, механизмах и мероприятиях, которые рекомендуется реализовать организациям и физическим лицам для защиты своих несовершеннолетних пользователей.

Рекомендации содержат рекомендации для следующих категорий сайтов и сервисов: "Обмен информацией между пользователями", "Информационные сайты", "Поисковые системы", "Интернет-сервисы" и "Ресурсы, содержащие информацию, запрещенную для детей".

Заместитель директора Департамента
Ж.В.САДОВНИКОВА

Приложение

МЕТОДИЧЕСКИЕ РЕКОМЕНДАЦИИ

ПО РЕАЛИЗАЦИИ МЕР, НАПРАВЛЕННЫХ НА ОБЕСПЕЧЕНИЕ БЕЗОПАСНОСТИ

ДЕТЕЙ В СЕТИ "ИНТЕРНЕТ"

Методические рекомендации по реализации мер, направленных на обеспечение безопасности детей в сети "Интернет" (далее - Рекомендации), разработаны на основе положений:

1. Федерального [закона от 29.12.2010 N 436-ФЗ](#) "О защите детей от информации, причиняющей вред их здоровью и развитию";
2. Концепции информационной безопасности детей, утвержденной [распоряжением Правительства Российской Федерации от 2 декабря 2015 г. N 2471-р](#);
3. рекомендаций парламентских слушаний "Актуальные вопросы обеспечения безопасности и развития детей в информационном пространстве", прошедших в Совете Федерации 17 апреля 2017 года;
4. международной практики деятельности государственных органов по обеспечению защиты детей от информации, причиняющей вред их здоровью и развитию, и саморегулированию в сети "Интернет".

Рекомендации направлены на расширение в Российской Федерации практики внедрения механизмов обеспечения информационной защиты несовершеннолетних пользователей организациями и физическими лицами, осуществляющими деятельность в информационно-телекоммуникационной сети "Интернет" (далее - организации и физические лица), посредством разработки и администрирования Интернет-ресурсов, сервисов и других технических программных решений.

Рекомендации носят рекомендательный характер и содержат:

1. принципы организации защиты несовершеннолетних пользователей, рекомендованные к руководству в повседневной работе организаций и физических лиц;
2. меры по организации защиты несовершеннолетних пользователей в сети "Интернет", включающие необходимые организационные мероприятия, перечень функций и опций сайтов и сервисов для детей и родителей (законных представителей).

Принципы обеспечения реализации комплекса мер, направленных на обеспечение безопасности детей в сети "Интернет"

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

1. Статьи 13, 17, 34 "Конвенции о правах ребенка" Генеральной Ассамблеи ООН обязывают государства-участников обеспечивать разработку "надлежащих принципов защиты ребенка от информации и материалов, наносящих вред его благополучию", а также устанавливать необходимые ограничения прав самого ребенка, включая "свободу искать, получать, передавать информацию и идеи любого рода". Статья 19 Конвенции закрепляет обязанность государств принимать "все необходимые законодательные, административные, социальные и просветительные меры с целью защиты ребенка от всех форм физического или психологического насилия, оскорбления или злоупотребления, отсутствия заботы или небрежного обращения, грубого обращения или эксплуатации, включая сексуальное злоупотребление, со стороны родителей, законных опекунов или любого другого лица, заботящегося о ребенке";
2. Статья 20 "Международного пакта о гражданских и политических правах" от 16 декабря 1966 г. предусматривает, что "всякая пропаганда войны", а также "всякое выступление в пользу национальной, расовой или религиозной ненависти, представляющее собой подстрекательство к дискриминации, вражде или насилию, должно быть запрещено законом";
3. Пункт 5 Статьи 9 Палермского Протокола от 15 ноября 2000 года предусматривает введение запрета на производство и оборот материалов, пропагандирующих преступления, связанные с торговлей людьми, включая пропаганду порнографии, эксплуатации проституции и иных коммерческих сексуальных услуг;
4. Статья 15 Модельного закона "Об основных гарантиях прав ребенка в государстве" N 14-9, принятого постановлением на четырнадцатом пленарном заседании Межпарламентской Ассамблеи государств - участников СНГ от 16 октября 1999 г., устанавливает основные гарантии защиты ребенка от информации, пропаганды и агитации, наносящих вред его здоровью, нравственному и духовному развитию. Закон обязывает органы государственной власти принимать меры по защите ребенка от информации, пропаганды и агитации, наносящих вред его здоровью, нравственному и духовному развитию, в том числе, от национальной, классовой, социальной нетерпимости, от рекламы алкогольной продукции и табачных изделий, от пропаганды социального, расового, национального и религиозного неравенства, а также от распространения печатной продукции, аудио- и видеопроизведений, пропагандирующей насилие и жестокость, порнографию, наркоманию, токсикоманию, антиобщественное поведение.

Примечание:

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

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

1. Федеральный [закон от 29 декабря 2010 г. N 436-ФЗ](#) "О защите детей от информации, причиняющей вред их здоровью и развитию", регулирующий отношения, связанные с защитой детей от информации, причиняющей вред их здоровью и (или) развитию, в том числе от такой информации, содержащейся в информационной продукции;
2. Федеральный закон от 3 июля 1998 г. N 124-ФЗ "Об основных гарантиях прав ребенка в Российской Федерации", устанавливающий обязанность органов государственной власти Российской Федерации принимать меры по защите ребенка от информации, пропаганды и агитации, наносящих вред его здоровью, нравственному и духовному развитию, в том числе от национальной, классовой, социальной нетерпимости, от рекламы алкогольной продукции и табачных изделий, от пропаганды социального, расового, национального и религиозного неравенства, от информации порнографического характера, от информации, пропагандирующей нетрадиционные сексуальные отношения, а также от распространения печатной продукции, аудио- и видеопроизведений, пропагандирующей насилие и жестокость, наркоманию, токсикоманию, антиобщественное поведение.

В соответствии с [приказом Минкомсвязи России от 16.06.2014 N 161](#) "Об утверждении требований к административным и организационным мерам, техническим и программно-аппаратным средствам защиты детей от информации, причиняющей вред их здоровью и (или) развитию", требования к административным и организационным мерам, техническим и программно-аппаратным средствам защиты детей от информации, причиняющей вред их здоровью и (или) развитию, применяются при обороте информационной продукции, содержащей информацию, запрещенную для распространения среди детей, в соответствии с частью 2 статьи 5 Федерального [закона от 29 декабря 2010 г. N 436-ФЗ](#) "О защите детей от информации, причиняющей вред их здоровью и развитию", в местах, доступных для детей, а также при предоставлении, в соответствии с частью 1 статьи 14 Федерального закона N 436-ФЗ доступа к информации, распространяемой посредством информационно-телекоммуникационных сетей, в том числе сети "Интернет", в местах, доступных для детей. При этом, в целях обеспечения информационной безопасности детей, организациям и физическим лицам рекомендуется реализовать комплекс административных и организационных мер, технических и программно-аппаратных средств защиты детей от информации, причиняющей вред их здоровью и (или) развитию.

Общие положения Методических рекомендаций

о реализации мер, направленных на обеспечение безопасности

детей в сети "Интернет"

Организациям и физическим лицам, осуществляющим деятельность в информационно-телекоммуникационной сети "Интернет", рекомендуется реализовать положения [приказа Минкомсвязи России от 16.06.2014 N 161](#) "Об утверждении требований к административным и организационным мерам, техническим и программно-аппаратным средствам защиты детей от информации, причиняющей вред их здоровью и (или) развитию" и нижеуказанный перечень административных мер защиты детей от информации, причиняющей вред их здоровью и (или) развитию:

1. Издавать нормативные локальные акты, направленные на обеспечение защиты детей от информации, причиняющей вред их здоровью и (или) развитию, и ознакомление с ними ответственных работников;
2. Осуществлять внутренний контроль за обновлением и соблюдением законодательства Российской Федерации о защите детей от информации, причиняющей вред их здоровью и (или) развитию, за соответствием применяемых административных и организационных мер защиты детей от информации, причиняющей вред их здоровью и (или) развитию, принципам и нормам информационной безопасности детей, включая критерии определения информационной продукции (информации), распространение которой на территории Российской Федерации запрещено или ограничено, установленные в действующих нормативных правовых актах Российской Федерации, в разъяснениях Верховного Суда Российской Федерации, а также общепризнанные нормы международного права, закрепленные в международных договорах Российской Федерации и рекомендациях международных организаций;
3. Обеспечивать оперативное рассмотрение претензий, жалоб или запросов органов власти, организаций и граждан Российской Федерации о нарушениях законодательства Российской Федерации о защите детей от информации, причиняющей вред их здоровью и (или) развитию, включая несоответствие применяемых административных и организационных мер защиты детей от информации, причиняющей вред их здоровью и (или) развитию, а также о наличии доступа детей к информации, запрещенной для распространения среди детей, и направление мотивированного ответа о результатах рассмотрения таких обращений, жалоб или претензий. В случае обращений со стороны органов власти, необходимо обеспечить предоставление информации и ответа в сроки, указанные в соответствующем обращении, но не позднее одного месяца с момента получения обращения;

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

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

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

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

Важным аспектом реализации административных мер защиты детей от информации, причиняющей вред их здоровью и (или) развитию, является повышение информационной компетентности в сфере кибербезопасности детей и их родителей (законных представителей). В связи с этим рекомендуется организациям и физическим лицам, осуществляющим деятельность в информационно-телекоммуникационной сети "Интернет", реализовывать следующие меры:

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

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

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

Обмен информацией между пользователями

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

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

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

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

4. Предоставить пользователям настройки предварительной модерации комментариев других пользователей перед публикацией в своем профиле;
5. Обеспечить внедрение функции, позволяющей ограничить взаимодействие детей с запрещенным для детей информационным контентом и включение данной функции по умолчанию;
6. Разработать механизм родительского контроля, предоставляющий возможность родителям отслеживать список друзей ребенка, его местонахождения и его активности;
7. Ограничить допуск детей в возрасте до 12 лет до каналов и сообществ, содержащих нежелательный контент для детей, и разработать механизмы предупреждения о нежелательном контенте для остальных возрастных групп до 18 лет в соответствии с возрастной классификацией информации, предусмотренной Федеральным [законом от 29 декабря 2010 г. N 436-ФЗ](#) "О защите детей от информации, причиняющей вред их здоровью и развитию";
8. Исключить для несовершеннолетних пользователей рекламу, ориентированную на вовлечение детей в противоправные действия и в политическую деятельность, и рекламу нежелательного контента для детей;
9. Разработать функционал, позволяющий авторам при публикации и распространении контента для более двух лиц разместить возрастную маркировку "запрещено для детей", и обеспечить невозможность просмотра данного материала несовершеннолетними пользователями;
10. Разработать правила для физических лиц и юридических лиц об использовании сайта или сервиса в качестве канала распространения информации для более двух пользователей, объединенных в группы, каналы и другие формы распространения информации.

Информационные сайты

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

1. Разместить знак информационной продукции и (или) текстовое предупреждение об ограничении ее распространения среди детей, соответствующие одной из категорий информационной продукции, установленных частью 3 статьи 6 Федерального [закона от 29 декабря 2010 г. N 436-ФЗ](#) "О защите детей от информации, причиняющей вред их здоровью и развитию";
2. До просмотра мультимедиа (видео, фотографии, комментарии и другого контента), в котором может содержаться запрещенная для детей информация, разместить текстовый или графический знак информационной продукции для предупреждения о недопустимости просмотра данного контента детьми;
3. При наличии функций, позволяющих пользователям обсуждать и комментировать контент, рядом с каждым сообщением должна быть предусмотрена функция жалобы в администрацию ресурса о нарушении законодательства в сфере информационной защиты детей.

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

Интернет-сервисы

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

1. При продаже товаров и услуг, которые включают информационный контент, запрещенный для детей и отдельных возрастных категорий в соответствии с Федеральным [законом от 29 декабря 2010 г. N 436-ФЗ](#) "О защите детей от информации, причиняющей вред их здоровью и развитию", администрация интернет-сервиса обязана запросить дополнительную информацию о покупателе (Ф.И.О.; возраст; телефон) и, в случае недостижения пользователем возраста продажи либо непредоставления данной информации, отказать в продаже товара или оказания услуг;
2. При предоставлении товаров и услуг, ориентированных на взрослых, подробная информация о них должна быть недоступна. Краткая информация должна содержать возрастную маркировку, текстовое предупреждение о недопустимости просмотра данного товара или услуги до момента согласия пользователя об ответственности за последствия просмотра подробной информации;

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

Поисковые системы

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

1. Разработать механизм предупреждения пользователей о нежелательном для детей контенте, выдающемся в результатах поиска;
2. Разработать механизм безопасного поиска, предназначенного для родителей (законных представителей) и позволяющего при включении ограничить допуск несовершеннолетних пользователей к нежелательному контенту;
3. Исключить из результатов поиска персональные данные детей в форме ссылок на аккаунты в социальных сетях;
4. Использовать средства контентной фильтрации для выявления запрещенной для детей информации.

Ресурсы, содержащие информацию, запрещенную для детей

В данную группу входят Интернет-ресурсы и технические программные решения, публикующие и распространяющие информационный контент, запрещенный для детей в соответствии с Федеральным [законом от 29 декабря 2010 г. N 436-ФЗ](#) "О защите детей от информации, причиняющей вред их здоровью и развитию" и отдельными законодательными актами Российской Федерации, которым рекомендуется реализовать следующие меры:

1. До ознакомления с информацией, публикуемой администрацией интернет-сервиса и запрещенной для детей в соответствии с Федеральным [законом от 29 декабря 2010 г. N 436-ФЗ](#) "О защите детей от информации, причиняющей вред их здоровью и развитию" и отдельными законодательными актами Российской Федерации, пользователь должен пройти регистрацию, указав Ф.И.О., номер телефона и возраст. Дальнейший доступ к информации должен быть разрешен только для совершеннолетних граждан, и, в случае недостижения пользователем совершеннолетнего возраста, администрация интернет-ресурса обязана отказать в регистрации и ограничить самостоятельный доступ к сайту. Организациям и физическим лицам рекомендуется исключить рекламу данных Интернет-ресурсов или технических программных решений, включая размещение информации об их работе, контенте и другой информации в сети "Интернет", для неограниченного круга лиц, среди которых могут быть несовершеннолетние пользователи.

**МИНИСТЕРСТВО ОБРАЗОВАНИЯ И НАУКИ РОССИЙСКОЙ
ФЕДЕРАЦИИ**

**ДЕПАРТАМЕНТ ГОСУДАРСТВЕННОЙ ПОЛИТИКИ В СФЕРЕ
ОБЩЕГО ОБРАЗОВАНИЯ**

ПИСЬМО

от 14 мая 2018 г. N 08-1184

О НАПРАВЛЕНИИ ИНФОРМАЦИИ

Департамент государственной политики в сфере общего образования Минобрнауки России направляет для сведения разработанные Временной комиссией Совета Федерации по развитию информационного общества методические рекомендации о размещении на информационных стендах, официальных интернет-сайтах и других информационных ресурсах общеобразовательных организаций и органов, осуществляющих управление в сфере образования, информации о безопасном поведении и использовании сети "Интернет".

Директор Департамента
А.Е.ПЕТРОВ

Приложение

МЕТОДИЧЕСКИЕ РЕКОМЕНДАЦИИ

О РАЗМЕЩЕНИИ НА ИНФОРМАЦИОННЫХ СТЕНДАХ, ОФИЦИАЛЬНЫХ

ИНТЕРНЕТ-САЙТАХ И ДРУГИХ ИНФОРМАЦИОННЫХ РЕСУРСАХ

ОБЩЕОБРАЗОВАТЕЛЬНЫХ ОРГАНИЗАЦИЙ И ОРГАНОВ, ОСУЩЕСТВЛЯЮЩИХ

УПРАВЛЕНИЕ В СФЕРЕ ОБРАЗОВАНИЯ, ИНФОРМАЦИИ О БЕЗОПАСНОМ

ПОВЕДЕНИИ И ИСПОЛЬЗОВАНИИ СЕТИ "ИНТЕРНЕТ"

Экспертами и членами Временной комиссии Совета Федерации по развитию информационного общества в рамках выполнения рекомендаций парламентских слушаний "Актуальные вопросы обеспечения безопасности и развития детей в информационном пространстве", которые прошли в Совете Федерации 17 апреля 2017 г., были разработаны методические рекомендации о размещении на информационных стендах, официальных интернет-сайтах и других информационных ресурсах общеобразовательных организаций и органов, осуществляющих управление в сфере образования, информации о безопасном поведении и использовании сети "Интернет" (далее - методические рекомендации).

Методические рекомендации направлены на качественное повышение уровня информационной деятельности общеобразовательных организаций и органов, осуществляющих управление в сфере образования, в части информирования учащихся, их родителей (законных представителей) и педагогических работников об основных аспектах информационной безопасности.

Методические рекомендации позволят общеобразовательным организациям и органам, осуществляющим управление в сфере образования, актуализировать уже используемые и размещенные информационные материалы, так и подготовить их в случае их отсутствия с учетом лучших практик и рекомендаций.

В рамках методических рекомендаций рассматриваются следующие инструменты:

1. информационные стенды;
2. официальные интернет-ресурсы;

3. средства массовой информации (школьные газеты, педагогические издания и другие).

Информационные стенды

На информационных стендах в общеобразовательных организациях, расположенных в фойе учреждений и в кабинетах, оснащенных персональными устройствами для выхода в сеть "Интернет", рекомендуется разместить информационные памятки, содержащие основные советы по обеспечению информационной безопасности учащихся.

В приложении N 1 к методическим рекомендациям представлен образец памятки для размещения на информационных стендах.

Средства массовой информации

В средствах массовой информации, ориентированных на обучающихся, рекомендуется в течение учебного года регулярно публиковать информационные материалы, посвященные отдельным аспектам информационной безопасности, а также различные памятки общего характера.

В средствах массовой информации, ориентированных на педагогическую общественность, рекомендуется в течение календарного года регулярно публиковать информационные материалы, посвященные отдельным аспектам информационной безопасности как несовершеннолетних, так и общеобразовательных организаций, а также различные памятки, обзоры нормативно-правового регулирования данной сферы и информацию о актуальных мероприятиях и событиях в данной сфере.

В ходе проведения Единого урока по безопасности в сети "Интернет" рекомендуется обеспечить выпуск тематического выпуска средства массовой информации либо серии публикаций, среди которых рассмотреть организованные мероприятия для обучающихся, их родителей (законных представителей) и педагогической общественности.

Официальные Интернет-ресурсы

Общеобразовательным организациям рекомендуется на своих официальных Интернет-ресурсах обеспечить функционирование самостоятельного и специализированного раздела "Информационная безопасность", в рамках которого предусмотреть размещение следующей информации:

№Раздел/подраздел	Формат представления материалов	Содержание материалов
Локальные нормативные акты в сфере обеспечения информационной безопасности 1.обучающихся	Копии документов в формате *PDF	Размещаются копии документов, т.е. сканированный вариант документа, соответствующий требованиям к параметрам сканирования. Размещаются документы, регламентирующие организацию и работу с персональными данными, планы мероприятий по обеспечению информационной безопасности обучающихся и другие. Публикуются актуальные сведения о федеральных и региональных законах, письмах органов власти и другие нормативно-правовые документы, регламентирующие обеспечение информационной безопасности несовершеннолетних. Допускается вместо копий размещать гиперссылки на соответствующие документы на сайтах органов государственной власти.
Нормативное 2.регулирование	Копии документов в формате *PDF Текст на странице сайта	Размещаются методические рекомендации и указывается информация о мероприятиях, проектах и программах, направленных на повышение информационной грамотности педагогических работников.
Педагогическим 3.работникам	Копии документов в формате *PDF	Размещается информационная памятка (приложение N 2) и указывается информация о мероприятиях, проектах и программах, направленных на повышение информационной грамотности обучающихся.
4.Обучающимся Родителям (законным представителям)	Текст на странице сайта	
5.обучающихся	Текст на странице сайта	Размещается информационная памятка (приложение N 3).

Размещается информация о рекомендуемых к использованию в учебном процессе безопасных сайтах, баннеры безопасных детских сайтов.

Текст на странице сайта

6. Детские безопасные сайты

Органам, осуществляющим управление в сфере образования, рекомендуется на своих официальных Интернет-ресурсах обеспечить функционирование самостоятельного и специализированного раздела "Информационная безопасность", в рамках которого предусмотреть размещение следующей информации:

Приложение N 1

ПАМЯТКА ДЛЯ ОБУЧАЮЩИХСЯ ОБ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ ДЕТЕЙ

НЕЛЬЗЯ

1. Всем подряд сообщать свою частную информацию (настоящие имя, фамилию, телефон, адрес, номер школы, а также фотографии свои, своей семьи и друзей);
2. Открывать вложенные файлы электронной почты, когда не знаешь отправителя;
3. Грубить, придирааться, оказывать давление - вести себя невежливо и агрессивно;
4. Не распоряжаться деньгами твоей семьи без разрешения старших - всегда спрашивай родителей;
5. Не встречайся с Интернет-знакомыми в реальной жизни - посоветуйся со взрослым, которому доверяешь.

ОСТОРОЖНО

1. Не все пишут правду. Читаешь о себе неправду в Интернете - сообщи об этом своим родителям или опекунам;
2. Приглашают переписываться, играть, обмениваться - проверь, нет ли подвоха;
3. Незаконное копирование файлов в Интернете - воровство;
4. Всегда рассказывай взрослым о проблемах в сети - они всегда помогут;
5. Используй настройки безопасности и приватности, чтобы не потерять свои аккаунты в соцсетях и других порталах.

МОЖНО

1. Уважай других пользователей;
2. Пользуешься Интернет-источником - делай ссылку на него;
3. Открывай только те ссылки, в которых уверен;
4. Общаться за помощью взрослым - родители, опекуны и администрация сайтов всегда помогут;
5. Пройди обучение на сайте "Сетевичок" и получи паспорт цифрового гражданина!

ИНФОРМАЦИОННАЯ ПАМЯТКА ДЛЯ ОБУЧАЮЩИХСЯ ДЛЯ РАЗМЕЩЕНИЯ НА ОФИЦИАЛЬНЫХ ИНТЕРНЕТ-РЕСУРСАХ

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

Компьютерные вирусы

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

Методы защиты от вредоносных программ:

1. Используй современные операционные системы, имеющие серьезный уровень защиты от вредоносных программ;
2. Постоянно устанавливай пачти (цифровые заплатки, которые автоматически устанавливаются с целью доработки программы) и другие обновления своей операционной системы. Скачивай их только с официального сайта разработчика ОС. Если существует режим автоматического обновления, включи его;
3. Работай на своем компьютере под правами пользователя, а не администратора. Это не позволит большинству вредоносных программ устанавливаться на твоём персональном компьютере;
4. Используй антивирусные программные продукты известных производителей, с автоматическим обновлением баз;
5. Ограничь физический доступ к компьютеру для посторонних лиц;
6. Используй внешние носители информации, такие как флешка, диск или файл из интернета, только из проверенных источников;
7. Не открывай компьютерные файлы, полученные из ненадежных источников. Даже те файлы, которые прислал твой знакомый. Лучше уточни у него, отправлял ли он тебе их.

Сети Wi-Fi

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

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

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

Советы по безопасности работы в общедоступных сетях Wi-fi:

1. Не передавай свою личную информацию через общедоступные Wi-Fi сети. Работая в них, желательно не вводить пароли доступа, логины и какие-то номера;
2. Используй и обновляй антивирусные программы и брандмауер. Тем самым ты обезопасишь себя от закачки вируса на твоё устройство;

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

4. Не используй публичный Wi-Fi для передачи личных данных, например для выхода в социальные сети или в электронную почту;

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

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

Социальные сети

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

Основные советы по безопасности в социальных сетях:

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

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

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

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

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

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

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

Электронные деньги

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

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

В России же они функционируют и о них уже прописано в законе, где их разделяют на несколько видов - анонимные и не анонимные. Разница в том, что анонимные - это те, в которых разрешается проводить операции без идентификации пользователя, а в неанонимных идентификация пользователя является обязательной.

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

Основные советы по безопасной работе с электронными деньгами:

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

2. Используй одноразовые пароли. После перехода на усиленную авторизацию тебе уже не будет угрожать опасность кражи или перехвата платежного пароля;
3. Выбери сложный пароль. Преступникам будет не просто угадать сложный пароль. Надежные пароли - это пароли, которые содержат не менее 8 знаков и включают в себя строчные и прописные буквы, цифры и несколько символов, такие как знак доллара, фунта, восклицательный знак и т.п. Например, \$tR0ng!;;
4. Не вводи свои личные данные на сайтах, которым не доверяешь.

Электронная почта

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

Основные советы по безопасной работе с электронной почтой:

1. Надо выбрать правильный почтовый сервис. В интернете есть огромный выбор бесплатных почтовых сервисов, однако лучше доверять тем, кого знаешь и кто первый в рейтинге;
2. Не указывай в личной почте личную информацию. Например, лучше выбрать "музыкальный_фанат@" или "рок2013" вместо "тема13";
3. Используй двухэтапную авторизацию. Это когда помимо пароля нужно вводить код, присылаемый по SMS;
4. Выбери сложный пароль. Для каждого почтового ящика должен быть свой надежный, устойчивый к взлому пароль;
5. Если есть возможность написать самому свой личный вопрос, используй эту возможность;
6. Используй несколько почтовых ящиков. Первый для частной переписки с адресатами, которым ты доверяешь. Это электронный адрес не надо использовать при регистрации на форумах и сайтах;
7. Не открывай файлы и другие вложения в письмах, даже если они пришли от твоих друзей. Лучше уточни у них, отправляли ли они тебе эти файлы;
8. После окончания работы на почтовом сервисе перед закрытием вкладки с сайтом не забудь нажать на "Выйти".

Кибербуллинг или виртуальное издевательство

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

Основные советы по борьбе с кибербуллингом:

1. Не бросайся в бой. Лучший способ: посоветоваться как себя вести и, если нет того, к кому можно обратиться, то вначале успокоиться. Если ты начнешь отвечать оскорблениями на оскорбления, то только еще больше разожжешь конфликт;
2. Управляй своей киберрепутацией;
3. Анонимность в сети мнимая. Существуют способы выяснить, кто стоит за анонимным аккаунтом;
4. Не стоит вести хулиганский образ виртуальной жизни. Интернет фиксирует все твои действия и сохраняет их. Удалить их будет крайне затруднительно;
5. Соблюдай свою виртуальную честь смолоду;
6. Игнорируй единичный негатив. Одноразовые оскорбительные сообщения лучше игнорировать. Обычно агрессия прекращается на начальной стадии;
7. Бан агрессора. В программах обмена мгновенными сообщениями, в социальных сетях есть возможность блокировки отправки сообщений с определенных адресов;

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

Мобильный телефон

Современные смартфоны и планшеты содержат в себе вполне взрослый функционал, и теперь они могут конкурировать со стационарными компьютерами. Однако, средств защиты для подобных устройств пока очень мало. Тестирование и поиск уязвимостей в них происходит не так интенсивно, как для ПК, то же самое касается и мобильных приложений.

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

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

Основные советы для безопасности мобильного телефона:

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

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

Необходимо обновлять операционную систему твоего смартфона;

Используй антивирусные программы для мобильных телефонов;

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

После того как ты выйдешь с сайта, где вводил личную информацию, зайти в настройки браузера и удалить cookies;

Периодически проверяй, какие платные услуги активированы на твоем номере;

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

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

Online игры

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

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

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

Основные советы по безопасности твоего игрового аккаунта:

1. Если другой игрок ведет себя плохо или создает тебе неприятности, заблокируй его в списке игроков;
2. Пожалуйся администраторам игры на плохое поведение этого игрока, желательно приложить какие-то доказательства в виде скриншотов;
3. Не указывай личную информацию в профайле игры;
4. Уважай других участников по игре;
5. Не устанавливай неофициальные патчи и моды;
6. Используй сложные и разные пароли;

7. Даже во время игры не стоит отключать антивирус. Пока ты играешь, твой компьютер могут заразить.

Фишинг или кража личных данных

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

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

Основные советы по борьбе с фишингом:

1. Следи за своим аккаунтом. Если ты подозреваешь, что твоя анкета была взломана, то необходимо заблокировать ее и сообщить администраторам ресурса об этом как можно скорее;
2. Используй безопасные веб-сайты, в том числе, интернет-магазинов и поисковых систем;
3. Используй сложные и разные пароли. Таким образом, если тебя взломают, то злоумышленники получат доступ только к одному твоему профилю в сети, а не ко всем;
4. Если тебя взломали, то необходимо предупредить всех своих знакомых, которые добавлены у тебя в друзьях, о том, что тебя взломали и, возможно, от твоего имени будет рассылаться спам и ссылки на фишинговые сайты;
5. Установи надежный пароль (PIN) на мобильный телефон;
6. Отключи сохранение пароля в браузере;
7. Не открывай файлы и другие вложения в письмах, даже если они пришли от твоих друзей. Лучше уточни у них, отправляли ли они тебе эти файлы.

Цифровая репутация

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

Твое место жительства, учебы, твое финансовое положение, особенности характера и рассказы о близких - все это накапливается в сети.

Многие подростки легкомысленно относятся к публикации личной информации в Интернете, не понимая возможных последствий. Ты даже не сможешь догадаться о том, что фотография, размещенная 5 лет назад, стала причиной отказа принять тебя на работу.

Комментарии, размещение твоих фотографий и другие действия могут не исчезнуть даже после того, как ты их удалишь. Ты не знаешь, кто сохранил эту информацию, попала ли она в поисковые системы и сохранилась ли она, а главное: что подумают о тебе окружающие люди, которые найдут и увидят это. Найти информацию много лет спустя сможет любой - как из добрых побуждений, так и с намерением причинить вред. Это может быть кто угодно.

Основные советы по защите цифровой репутации:

1. Подумай, прежде чем что-то публиковать и передавать у себя в блоге или в социальной сети;
2. В настройках профиля установи ограничения на просмотр твоего профиля и его содержимого, сделай его только "для друзей";
3. Не размещай и не указывай информацию, которая может кого-либо оскорблять или обижать.

Авторское право

Современные школьники - активные пользователи цифрового пространства. Однако далеко не все знают, что пользование многими возможностями цифрового мира требует соблюдения прав на интеллектуальную собственность.

Термин "интеллектуальная собственность" относится к различным творениям человеческого ума, начиная с новых изобретений и знаков, обозначающих собственность на продукты и услуги, и заканчивая книгами, фотографиями, кинофильмами и музыкальными произведениями.

Авторские права - это права на интеллектуальную собственность на произведения науки, литературы и искусства. Авторские права выступают в качестве гарантии того, что интеллектуальный/творческий труд автора не будет напрасным, даст ему справедливые возможности заработать на результатах своего труда, получить известность и признание. Никто без разрешения автора не может воспроизводить его произведение, распространять, публично демонстрировать, продавать, импортировать, пускать в прокат, публично исполнять, показывать/исполнять в эфире или размещать в Интернете.

Использование "пиратского" программного обеспечения может привести к многим рискам: от потери данных к твоим аккаунтам до блокировки твоего устройства, где установлена нелегальная программа. Не стоит также забывать, что существуют легальные и бесплатные программы, которые можно найти в сети.

О портале

Сетевичок.рф - твой главный советчик в сети. Здесь ты можешь узнать о безопасности в сети понятным и доступным языком, а при возникновении критической ситуации обратиться за советом. А также принять участие в конкурсах и стать самым цифровым гражданином!

Приложение N 3

ПАМЯТКА ДЛЯ РОДИТЕЛЕЙ ОБ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ ДЕТЕЙ

Определение термина "информационная безопасность детей" содержится в Федеральном законе N 436-ФЗ "О защите детей от информации, причиняющей вред их здоровью и развитию", регулирующим отношения, связанные с защитой детей от информации, причиняющей вред их здоровью и (или) развитию. Согласно данному закону "информационная безопасность детей" - это состояние защищенности, при котором отсутствует риск, связанный с причинением информацией вреда их здоровью и (или) физическому, психическому, духовному, нравственному развитию.

В силу Федерального закона N 436-ФЗ информацией, причиняющей вред здоровью и (или) развитию детей, является:

1. информация, запрещенная для распространения среди детей;
2. информация, распространение которой ограничено среди детей определенных возрастных категорий.
3. К информации, запрещенной для распространения среди детей, относится:
4. информация, побуждающая детей к совершению действий, представляющих угрозу их жизни и (или) здоровью, в т.ч. причинению вреда своему здоровью, самоубийству;
5. способность вызвать у детей желание употребить наркотические средства, психотропные и (или) одурманивающие вещества, табачные изделия, алкогольную и спиртосодержащую продукцию, пиво и напитки, изготавливаемые на его основе; принять участие в азартных играх, заниматься проституцией, бродяжничеством или попрошайничеством;
6. обосновывающая или оправдывающая допустимость насилия и (или) жестокости либо побуждающая осуществлять насильственные действия по отношению к людям и животным;
7. отрицающая семейные ценности и формирующая неуважение к родителям и (или) другим членам семьи;
8. оправдывающая противоправное поведение;
9. содержащая нецензурную брань;
10. содержащая информацию порнографического характера.

К информации, распространение которой ограничено среди детей определенного возраста, относится:

1. информация, представляемая в виде изображения или описания жестокости, физического и (или) психического насилия, преступления или иного антиобщественного действия;
2. вызывающая у детей страх, ужас или панику, в т.ч. представляемая в виде изображения или описания в унижающей человеческое достоинство форме ненасильственной смерти, заболевания, самоубийства, несчастного случая, аварии или катастрофы и (или) их последствий;
3. представляемая в виде изображения или описания половых отношений между мужчиной и женщиной;
4. содержащая бранные слова и выражения, не относящиеся к нецензурной брани.

С учетом этого Вам предлагаются правила работы в сети Интернет для различных возрастных категорий, соблюдение которых позволит обеспечить информационную безопасность ваших детей.

Общие правила для родителей

1. Независимо от возраста ребенка используйте программное обеспечение, помогающее фильтровать и контролировать информацию, но не полагайтесь полностью на него. Ваше внимание к ребенку - главный метод защиты.
2. Если Ваш ребенок имеет аккаунт на одном из социальных сервисов (LiveJournal, blogs.mail.ru, vkontakte.ru и т.п.), внимательно изучите, какую информацию помещают его участники в своих профилях и блогах, включая фотографии и видео.
3. Проверьте, с какими другими сайтами связан социальный сервис Вашего ребенка. Странички Вашего ребенка могут быть безопасными, но могут и содержать ссылки на нежелательные и опасные сайты (например, порносайт, или сайт, на котором друг упоминает номер сотового телефона Вашего ребенка или Ваш домашний адрес)
4. Поощряйте Ваших детей сообщать обо всем странном или отталкивающем и не слишком остро реагируйте, когда они это делают (из-за опасения потерять доступ к Интернету дети не говорят родителям о проблемах, а также могут начать использовать Интернет вне дома и школы).
5. Будьте в курсе сетевой жизни Вашего ребенка. Интересуйтесь, кто их друзья в Интернет так же, как интересуетесь реальными друзьями.

Возраст от 7 до 8 лет

В Интернете ребенок старается посетить те или иные сайты, а возможно и чаты, разрешение на посещение которых он не получил бы от родителей. Поэтому родителям особенно полезны будут те отчеты, которые предоставляются программами по ограничению использования Интернета, т.е. Родительский контроль или то, что вы сможете увидеть во временных файлах. В результате, у ребенка не будет ощущения, что за ним ведется постоянный контроль, однако, родители будут по-прежнему знать, какие сайты посещает их ребенок. Дети в данном возрасте обладают сильным чувством семьи, они доверчивы и не сомневаются в авторитетах. Они любят играть в сетевые игры и путешествовать по Интернету, используя электронную почту, заходить на сайты и чаты, не рекомендованные родителями.

Советы по безопасности в сети Интернет для детей 7 - 8 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 специальные детские поисковые машины.
5. Используйте средства блокирования нежелательного контента как дополнение к стандартному Родительскому контролю.
6. Создайте семейный электронный ящик, чтобы не позволить детям иметь собственные адреса.

7. Блокируйте доступ к сайтам с бесплатными почтовыми ящиками с помощью соответствующего программного обеспечения.
8. Приучите детей советоваться с Вами перед опубликованием какой-либо информации средствами электронной почты, чатов, регистрационных форм и профилей.
9. Научите детей не загружать файлы, программы или музыку без вашего согласия.
10. Не разрешайте детям использовать службы мгновенного обмена сообщениями.
11. В "белый" список сайтов, разрешенных для посещения, вносите только сайты с хорошей репутацией.
12. Не забывайте беседовать с детьми об их друзьях в Интернете, как если бы речь шла о друзьях в реальной жизни.
13. Не делайте "табу" из вопросов половой жизни, так как в Интернете дети могут легко наткнуться на порнографию или сайты "для взрослых".
14. 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.

Возраст детей от 9 до 12 лет

В данном возрасте дети, как правило, уже слышали о том, какая информация существует в Интернете. Совершенно нормально, что они хотят это увидеть, прочесть, услышать. При этом нужно помнить, что доступ к нежелательным материалам можно легко заблокировать при помощи средств Родительского контроля.

Советы по безопасности для детей от 9 до 12 лет

1. Создайте список домашних правил посещения Интернет при участии детей и требуйте его выполнения.
2. Требуйте от Вашего ребенка соблюдения норм нахождения за компьютером.
3. Наблюдайте за ребенком при работе за компьютером, покажите ему, что Вы беспокоитесь о его безопасности и всегда готовы оказать ему помощь.
4. Компьютер с подключением в Интернет должен находиться в общей комнате под присмотром родителей.
5. Используйте средства блокирования нежелательного контента как дополнение к стандартному Родительскому контролю.
6. Не забывайте принимать непосредственное участие в жизни ребенка, беседовать с детьми об их друзьях в Интернете.
7. Настаивайте, чтобы дети никогда не соглашались на личные встречи с друзьями по Интернету.
8. Позволяйте детям заходить только на сайты из "белого" списка, который создайте вместе с ними.
9. 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.
10. Приучите детей не загружать программы без Вашего разрешения. Объясните им, что они могут случайно загрузить вирусы или другое нежелательное программное обеспечение.
11. Создайте Вашему ребенку ограниченную учетную запись для работы на компьютере.
12. Приучите Вашего ребенка сообщать вам о любых угрозах или тревогах, связанных с Интернетом. Напомните детям, что они в безопасности, если сами рассказали вам о своих тревогах и опасениях.
13. Расскажите детям о порнографии в Интернете.

14. Настаивайте на том, чтобы дети предоставляли вам доступ к своей электронной почте, чтобы вы убедились, что они не общаются с незнакомцами.

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

Возраст детей от 13 до 17 лет

В этом возрасте подростки активно используют поисковые машины, пользуются электронной почтой, службами мгновенного обмена сообщениями, скачивают музыку и фильмы. Мальчикам в этом возрасте больше по нраву сметать все ограничения, они жаждут грубого юмора, азартных игр, картинок "для взрослых". Девочки предпочитают общаться в чатах, при этом они гораздо более чувствительны к сексуальным домогательствам в Интернете.

Зачастую в данном возрасте родителям уже весьма сложно контролировать своих детей, так как об Интернете они уже знают значительно больше своих родителей. Тем не менее, не отпускайте детей в "свободное плавание" по Интернету. Старайтесь активно участвовать в общении ребенка в Интернете.

Важно по-прежнему строго соблюдать правила Интернет-безопасности - соглашение между родителями и детьми. Кроме того, необходимо как можно чаще просматривать отчеты о деятельности детей в Интернете. Следует обратить внимание на необходимость содержания родительских паролей (паролей администраторов) в строгом секрете и обратить внимание на строгость этих паролей.

Советы по безопасности в этом возрасте от 13 до 17 лет

1. Создайте список домашних правил посещения Интернета при участии подростков и требуйте безусловного его выполнения. Обговорите с ребенком список запрещенных сайтов ("черный список"), часы работы в Интернете, руководство по общению в Интернете (в том числе в чатах).

2. Компьютер с подключением к сети Интернет должен находиться в общей комнате.

3. 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.

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

5. Необходимо знать, какими чатами пользуются Ваши дети. Поощряйте использование модерлируемых чатов и настаивайте, чтобы дети не общались в приватном режиме.

6. Настаивайте на том, чтобы дети никогда не встречались лично с друзьями из сети Интернет.

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

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

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

10. Расскажите детям о порнографии в Интернете. Помогите им защититься от спама. Научите подростков не выдавать в Интернете своего реального электронного адреса, не отвечать на нежелательные письма и использовать специальные почтовые фильтры.

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

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

13. Объясните детям, что ни в коем случае нельзя использовать Сеть для хулиганства, распространения сплетен или угроз другим людям.

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

Постоянно контролируйте использование Интернета Вашим ребенком! Это не нарушение его личного пространства, а мера предосторожности и проявление Вашей родительской ответственности и заботы.