

**Министерство образования Иркутской области
ГКУ «Центр профилактики, реабилитации и коррекции»**



МЕТОДИЧЕСКИЕ РЕКОМЕНДАЦИИ

**Профилактика вовлечения несовершеннолетних посредством сети
«Интернет» в противоправную деятельность.**

**Профилактика бесконтрольного использования
личных мобильных устройств во время образовательного процесса.**



Иркутск, 2022

Печатается по решению редакционно-издательского совета

Авторы-составители: Галстян М.Н., Дичина Н.Ю., Старкова А.П.
Методические рекомендации. Профилактика вовлечения несовершеннолетних посредством сети «Интернет» в противоправную деятельность. Профилактика бесконтрольного использования личных мобильных устройств во время образовательного процесса. Иркутск, ЦПРК-2022, с.67

Методические рекомендации адресованы руководителям, педагогам, ответственным лицам за обеспечение информационной безопасности образовательных организаций.

Методические рекомендации помогут специалистам актуализировать и дополнить свои представления о нормативно-правовых основах обеспечения информационной безопасности в образовательной среде, профилактике вовлечения несовершеннолетних посредством сети «Интернет» в противоправную деятельность, причиняющую вред их здоровью, профилактике бесконтрольного использования личных мобильных устройств несовершеннолетних во время образовательного процесса.

Содержание

Введение	4
Деятельность образовательной организации по профилактике Интернет -рисков и угроз среди детей и подростков	7
Деятельность образовательной организации по профилактике бесконтрольного использования личных мобильных устройств несовершеннолетних во время образовательного процесса	14
Заключение	16
Литература	24
Приложения	25
Приложение 1. Нормативно-правовое обеспечение информационной безопасности образовательной среды	27
Приложение 2. Образцы локальных актов образовательной организации в области информационной безопасности детей	30
<i>Приказ «Об организации информационной безопасности в образовательной организации»</i>	30
<i>Положение об ограничении доступа обучающихся к видам информации, распространяемой посредством сети «Интернет», причиняющей вред здоровью и (или) развитию детей, а также не соответствующей задачам образования</i>	32
<i>План мероприятий по обеспечению информационной безопасности обучающихся на 2019-2022 годы</i>	35
<i>Формулировки для внесения изменений в должностные инструкции педагогических работников и иных работников образовательной организации об ограничении доступа обучающихся к видам информации, распространяемой посредством сети «Интернет», причиняющей вред здоровью и (или) развитию детей, а также не соответствующей задачам образования</i>	38
<i>Примерный акт установки системы контентной фильтрации в образовательном учреждении</i>	40
<i>Формы:</i>	41
<i>Акт проверки контентной фильтрации в образовательной организации;</i>	
<i>Журнал контроля контентной фильтрации;</i>	
<i>Журнал регистрации случаев обнаружения сайтов;</i>	
<i>График работы точки доступа к сети Интернет;</i>	
<i>Журнал учета доступа в сеть Интернет.</i>	
<i>Формы и перечень листов ознакомления:</i>	45
<i>для сотрудников с инструкцией ОУ о порядке действий при осуществлении контроля над использованием обучающимися сети Интернет;</i>	
<i>сотрудников ОУ с правилами использования сети Интернет в образовательной организации;</i>	
<i>учащихся ОУ с правилами использования сети Интернет в образовательной организации.</i>	
Приложение 3. Перечень рекомендуемой методической литературы для использования заинтересованными лицами и организациями	46
Приложение 4. Перечень рекомендуемых сайтов в сети «Интернет» для использования заинтересованными лицами и организациями	54
Приложение 5. Памятки, полезные советы, правила для обучающихся, родителей и педагогических работников «Безопасный интернет»	60
Приложение 6. Памятки, полезные советы, правила для обучающихся, родителей и педагогических работников по профилактике неблагоприятных для здоровья и обучения детей эффектов от воздействия устройств мобильной связи	63

Введение

Современную жизнь невозможно представить без Интернета. Цифровые технологии открывают безграничные возможности в сфере развития и образования детей. Образовательная среда является открытой системой, отражающей все закономерности и тенденции развития окружающей социальной среды, в том числе и проблемы, характерные для современного общества.

Активное использование интернета существенно меняет социальные и культурные практики, в первую очередь, у наиболее активных пользователей цифровых технологий — детей, подростков и молодежи. Интернет становится пространством не только возможностей, но и рисков, в том числе, рисков деструктивного и аутодеструктивного поведения.

Актуальным и значимым становится поиск решений проблем воздействия информации, которая может нанести вред здоровью и развитию детей, а также других социально-негативных условий, формирующих деструктивное поведение.

Стремительность изменений социальной жизни снижает психологический ресурс сопротивляемости детей и молодежи негативным воздействиям среды, способствует распространению различных форм отклоняющегося поведения. Повышение частоты их проявления внутри образовательной среды, появление интернет-технологий как новой реальности, где снижен уровень социального контроля, – все это требует поиска новых психолого-педагогических технологий поддержки и сопровождения обучающихся. Таким образом, существенным и всё более актуальным признаком качественной образовательной среды является её безопасность, в том числе информационная безопасность.

Термин «информационная безопасность» используется для обозначения двух различных понятий. В первом случае, информационная безопасность рассматривается как практика предотвращения несанкционированного доступа, использования, раскрытия, искажения, изменения, исследования, записи или уничтожения информации. Это универсальное понятие применяется вне зависимости от формы, которую могут принимать данные (электронная или, например, физическая).

Основная задача обеспечения информационной безопасности в данном контексте — сбалансированная защита конфиденциальности, целостности и доступности данных, с учетом целесообразности применения и без какого-либо ущерба производительности организации.

Таким образом, речь идет о защите информации, о мерах, которые принимает образовательная организация по защите разных видов информации. Актуальность данного направления работы определяется увеличением числа угроз, связанных с цифровизацией и информатизацией системы образования, широким использованием дистанционных технологий, наличием противоречия между требуемой и имеющейся квалификацией

специалистов, отвечающих за обеспечение информационной безопасности в образовательных организациях.

Также понятие «информационная безопасность» используется при обсуждении проблем безопасности обучающихся. В данном случае информационная безопасность рассматривается как «состояние защищенности детей, при котором отсутствует риск, связанный с причинением информацией вреда их здоровью и (или) физическому, психическому, духовному, нравственному развитию»¹.

С позиций личностно-ориентированного подхода (Есенкожа Е.М., Касен Г.В., 2015, Солдатов Г.В., Рассказова Е.И., 2012) информационная безопасность определяется как состояние защищенности личности, обеспечивающее ее целостность как активного социального субъекта и возможности развития в условиях информационного взаимодействия с окружающей средой.

Данный подход предполагает использование педагогических и психологических средств для развития информационной культуры, медиаграмотности и «саногенного» мышления и поведения обучающихся, а также для развития личностных качеств, способствующих противостоянию аддиктивному поведению и вовлечению в экстремистские и иные опасные группы и сообщества. Данный подход сочетается с неспецифической первичной профилактикой, включая разнообразные воспитательные и психологические мероприятия, развивающие навыки общения; «интеграцию виртуального и реального миров», когда подростки рассказывают друг другу и взрослым о своей жизни в интернете, а так же встречаются и общаются со своими виртуальными друзьями в реальности; включение подростков в различные реальные группы и содействие преодолению чувства одиночества; поддержку в преодолении трудностей в учебной деятельности, в общении и взаимодействии и т.п.

Актуальность задач образовательной организации, связанных с защитой детей от негативного влияния информации связана с возрастанием числа и спектра угроз, сопряженных с воздействием разных источников информации, формированием феномена «информационной социализации».

Существенным концептуальным направлением профилактической деятельности является отказ от ее экстенсивного расширения, от увеличения числа мероприятий по профилактике отдельных видов рисков (аддиктивного, суицидального и т.п. поведения) в пользу выстраивания системной работы, направленной на формирование субъектной позиции несовершеннолетних по отношению к рискам и угрозам любого рода и развитие ресурсов устойчивости несовершеннолетних к их воздействию. Ключевым направлением профилактической работы должно стать развитие ресурсов устойчивости детей и подростков к Интернет-рискам и угрозам.

¹ Федеральный закон от 29 декабря 2010 г. N 436-ФЗ «О защите детей от информации, причиняющей вред их здоровью и развитию» // Российская газета – Федеральный выпуск № 5376 (297). 31.12.2010

Специалистами ГКУ «Центр профилактики, реабилитации и коррекции», на основе открытых источников: правительственных сайтов, публикаций в прессе, методической и справочной литературы сделан обзор материалов, проанализирован, обобщен, и систематизирован (международный, федеральный и региональный) опыт по данному вопросу.

Предложенные методические рекомендации помогут педагогическим работникам актуализировать и дополнить свои представления о нормативно-правовых основах обеспечения информационной безопасности в образовательной среде, профилактике вовлечения несовершеннолетних посредством сети «Интернет» в противоправную деятельность, причиняющую вред их здоровью, профилактике бесконтрольного использования личных мобильных устройств несовершеннолетних во время образовательного процесса.

Деятельность образовательной организации по профилактике Интернет - рисков и угроз среди детей и подростков



Риски и угрозы, с которыми сталкивается сегодня несовершеннолетний в Сети, многообразны. Наряду с угрозами развития Интернет-зависимости, увлеченности детей играми в Интернете, угрозами финансовых махинаций, сегодня набирают обороты новые угрозы, связанные с общением в социальных сетях, свидетельствующие о целенаправленном разрушающем воздействии на незрелую психику школьников: это и вопиющие случаи массовых суицидов школьников - членов одних и тех же групп в социальных сетях, и проблемы кибербуллинга и груминга в сети, проблемы рекрутинга в закрытые сообщества, включая экстремистские и иные опасные группы и т.п.²

Сегодня, по данным Института развития Интернета, им пользуются 76% россиян. Растет и число школьников, ежедневно использующих социальные сети. Результаты мониторинга Фонда «Национальные ресурсы образования», проведенного среди 2 500 школьников от 13 до 18 лет в 84 регионах России, показывают, что 50% ребят заходят в социальные сети более девяти раз в день. Чаще всего школьники используют социальные сети для переписки с друзьями — 83%, для чтения постов и просмотра новостной ленты — 74%, для прослушивания музыки — 70%, для размещения фотографий — 26%.

По данным индекса цифровой культуры Microsoft за 2018 год, Россия заняла 19-е место в мире из 22 возможных по уровню подверженности рискам — в 2018 году онлайн-рискам подверглись 74% россиян. Второй год подряд самым распространенным стал риск нежелательной коммуникации (67%). Часто риски проявлялись в форме оскорблений и недостоверной информации в Сети. Две трети россиян сталкивались с оскорблениями, практически 40% — с недостоверной информацией и фейк-ньюз; каждый пятый пострадал от действий финансовых мошенников. Этим рискам подвержены не только взрослые, но и подростки и даже дети младшего школьного возраста.

В 2017 году в ходе опроса Фонда «Национальные ресурсы образования» о наличии в сети Интернет-угроз для несовершеннолетних высказались 93% из 5 тысяч респондентов. По их мнению, подростки становятся жертвами мошеннических действий, сталкиваются с



² ФГБНУ «Центр защиты прав и интересов детей», 2018. — 11 с.

нежелательным для психологического развития содержанием, принимают за истину ложную информацию, а также порой неумышленно, по незнанию, сами совершают в сети противоправные действия.

Эти данные подтверждаются и статистикой МВД. Только за период с января по ноябрь 2018 года было зарегистрировано более 156 тысяч преступлений, совершенных с использованием компьютерных и телекоммуникационных технологий. Среди них более 38 тысяч преступлений совершены самими несовершеннолетними, около 1,5 тысяч несовершеннолетних были вовлечены в совершение преступлений или антиобщественных действий.

В настоящее время в мире уже возникло устойчивое понимание того, что проблема детской безопасности в Интернете – это предмет, требующий скоординированного решения на всех уровнях: от семейного и муниципального до регионального и международного. В решении этой проблемы необходимо действовать системно и использовать не только правовые регуляторы, но и нормы обычаев и морали, а также технические и технологические возможности.



В целях содействия более безопасному и ответственному пользованию интернетом и другими онлайн технологиями, особенно детьми и молодыми людьми, в 2004 году Европейской Комиссией был учрежден День Безопасного Интернета, а также разработана и принята многолетняя программа по защите детей и молодежи от вредного и противоправного содержания сети интернет. Программа направлена на поддержку таких направлений, как обеспечение осведомленности общественности по заявленной проблеме; распространение информации о возможных рисках, связанных с использованием интернет-технологий; информирование о последних технических новинках, обеспечивающих безопасное пребывание в режиме онлайн; борьба с незаконным контентом и противоправным поведением в интернете; содействие развитию безопасного киберпространства; создание базы статистических и аналитических данных, поощрение скоординированного подхода для исследований в соответствующих областях.

Довольно острое положение с созданием и распространением в Рунете контента, объективно опасного для несовершеннолетних, привело к усилению внимания общества и профессионалов к проблеме защиты детей от негативных и противоправных действий, совершаемых с использованием «высоких технологий» и Интернета, в частности.

15 августа 2008 года при участии Общественной палаты РФ в нашей стране начал работу Национальный Узел Интернет-безопасности в России – центр общественной и профессиональной деятельности по повышению уровня защищенности детей от опасностей интернета. Национальный Узел

проводит информационную, просветительскую и аналитическую деятельность по данному вопросу, а его сотрудники оказывают адресные консультации и помощь жертвам интернет-преступлений. В рамках работы Национального Узла был реализован общественный механизм по выявлению противоправного контента, объективно представляющего угрозу для детей, в форме горячей линии по противоправному контенту.

Для того чтобы решить проблемы информационной безопасности Российской Федерации, была сформирована и принята Доктрина информационной безопасности РФ 2016 (Указ Президента РФ от 05.12.2016 № 646 «Об утверждении Доктрины информационной безопасности Российской Федерации»). В этом документе информационная безопасность страны рассматривается в качестве состояния защищенности человека, социума и государства от информационных угроз внутреннего и внешнего характера, в ходе которого осуществляются конституционные права и свободы личности, высокое качество жизнедеятельности граждан, независимость, территориальная целостность и поступательное общественно-экономическое развитие страны, ее оборона и безопасность.

Создание безопасной информационно-образовательной среды, в современных условиях, когда количество информации, влияющей на формирование внутренней позиции обучающихся, увеличивается ежегодно в геометрической прогрессии, является актуальной проблемой, необходимость разрешения которой отражена в стратегических документах сферы образования: Федеральный государственный образовательный стандарт общего образования, Государственная программа Российской Федерации «Развитие образования», Стратегия развития воспитания в Российской Федерации на период до 2025 года и иные нормативно-правовые документы (приложение 1).

С 2006 года федеральными органами государственной власти Российской Федерации осуществляется целенаправленная деятельность, связанная с ограничением в образовательных организациях доступа обучающихся к негативной информации.

Далее рассмотрим основополагающие ведомственные документы по основам информационной безопасности в образовательных организациях.



Методические рекомендации по основам информационной безопасности для обучающихся общеобразовательных организаций с учётом информационных, потребительских, технических и коммуникативных аспектов информационной безопасности

<https://www.единыйурок.рф/images/doc/metod/cyber.pdf>

Методические рекомендации разработаны Временной комиссией Совета Федерации по развитию информационного общества совместно с ФСБ России, Минобрнауки России, Минкомсвязи России, Роскомнадзором, МЧС России и Минздравом России.

Задачи методических рекомендаций:

оказание методической поддержки педагогических работников и сотрудников образовательных организаций России с целью организации обучения детей и их родителей (законных представителей) информационной безопасности;

использование современных технологий и методик в организации обучения детей, в частности в рамках межпредметного обучения, внеурочной деятельности и других форм обучения;

повышение уровня информационной грамотности педагогических работников и сотрудников администрации общеобразовательных организаций Российской Федерации в части тематических положений приказа Министерства труда и социальной защиты РФ от 18 октября 2013 г. N 544н «Об утверждении профессионального стандарта «Педагог (педагогическая деятельность в сфере дошкольного, начального общего, основного общего, среднего общего образования) (воспитатель, учитель)», ФГОС ООО, ФГОС НОО и ФГОС СОО;

оказать методическую помощь администрациям субъектов Российской Федерации, органам местного самоуправления и администрациям образовательных организаций в организации обучения детей, их родителей (законных представителей) и педагогических работников информационной безопасности;

формирование тем и вопросов по вопросам информационной безопасности для включения в тематические учебники, учебные пособия и другие учебно-методические материалы.

Методические рекомендации направлены на организацию обучения детей по следующим направлениям:

1. Организация обучения в рамках действующих учебных предметов и(или) использования межпредметного обучения;

2. Организация обучения в рамках части основной образовательной программы, формируемой участниками образовательного процесса, включая организацию отдельных учебных предметов, учебных курсов и внеурочную деятельность;

3. Организация обучения в рамках дополнительного образования.

Методические рекомендации ориентированы на следующие аудитории: учителя, преподаватели и классные руководители; сотрудники администрации образовательных организаций по учебно-воспитательной работе, по воспитательной работе и безопасности образовательного процесса и обучающихся; ответственные лица в штате образовательных организаций в части психологического и воспитательного взаимодействия с обучающимися и педагогами (педагоги-организаторы, психологи, методисты и другие сотрудники образовательных организаций); ответственные лица в штате образовательных организаций в части дополнительного образования обучающихся и организации внеурочной деятельности.

Методические рекомендации содержат общие представления о сферах безопасности в информационном пространстве и мерах, которые реализуются в образовательной среде для обеспечения информационной безопасности обучающихся.



Методические рекомендации по ограничению в образовательных организациях доступа обучающихся к видам информации, распространяемой посредством сети «Интернет», причиняющей вред здоровью и (или) развитию детей, а также не соответствующей задачам образования³

(утв. Министерством просвещения РФ, Министерством цифрового развития, связи и массовых коммуникаций РФ, Федеральной службой по надзору в сфере связи, информационных технологий и массовых коммуникаций 16 мая 2019 года)

<https://www.garant.ru/products/ipo/prime/doc/72145832/>

Методические рекомендации разработаны Временной комиссией Совета Федерации по развитию информационного общества совместно с Министерством просвещения Российской Федерации, Министерством цифрового развития, связи и массовых коммуникаций Российской Федерации и Федеральной службой по надзору в сфере связи, информационных технологий и массовых коммуникаций, рамках реализации пункта 7 плана мероприятий по реализации Концепции информационной безопасности детей на 2018 - 2020 годы, утверждённого приказом Минкомсвязи России от 27 февраля 2018г. N88. Методические рекомендации прошли общественное обсуждение с участием 10135 педагогических работников на площадке Экспертного совета по информатизации системы образования и воспитания при Временной комиссии Совета Федерации по развитию информационного общества.

Методические рекомендации актуализируют различные аспекты и дополняют методические рекомендации по ограничению в образовательных организациях доступа обучающихся к видам информации, распространяемой посредством сети «Интернет», причиняющей вред здоровью и (или) развитию детей, а также не соответствующей задачам образования, направленные Минобрнауки России письмом от 28.04.2014 N ДЛ-115/03 в адрес субъектов Российской Федерации с учетом изменений законодательства и анализа правоприменительной деятельности.

Методические рекомендации распространяются на учреждения для детей-сирот и детей, оставшихся без попечения родителей; общеобразовательные организации; организации дополнительного образования; организации и индивидуальные предприниматели, осуществляющие образовательную деятельность по программам основного и дошкольного образования; дошкольные образовательные организации; профессиональные образовательные организации. Методические

³ Письмо Минпросвещения России от 29 марта 2019 года № 03-393

рекомендации не распространяются на образовательные организации высшего образования и организации дополнительного профессионального образования.

Документ представляют собой перечень рекомендаций о различных мерах, механизмах и мероприятиях, которые рекомендуется реализовать организациям и физическим лицам для защиты своих несовершеннолетних пользователей, и содержит рекомендации для следующих категорий сайтов и сервисов: «Обмен информацией между пользователями», «Информационные сайты», «Поисковые системы», «Интернет-сервисы» и «Ресурсы, содержащие информацию, запрещенную для детей».

Образцы локальных актов образовательной организации в области информационной безопасности детей предложены в приложении №2.



Методические рекомендации для общеобразовательных организаций по вопросам обработки персональных данных (письмо Министерства цифрового развития, связи и массовых коммуникаций РФ от 28 августа 2020г. №ЛБ-С-074-24059 «О методических рекомендациях»)

<https://www.garant.ru/products/ipo/prime/doc/74485566/#1000>

Подготовлены рабочей группой по вопросам совершенствования государственной политики в сфере развития информационного общества Комитета Совета Федерации по конституционному законодательству, Минкомсвязь России, Минпросвещения России и Роскомнадзор в целях оказания методической поддержки администрациям общеобразовательных организаций по соблюдению требований законодательства Российской Федерации в области персональных данных при обработке персональных данных несовершеннолетних, их родителей (законных представителях) и работников общеобразовательной организации.

На основе методических рекомендаций организована дистанционная программа повышения квалификации «Обработка персональных данных в образовательных организациях» на площадке Экспертной группы по образованию рабочей группы по вопросам совершенствования государственной политики в сфере развития информационного общества Комитета Совета Федерации по конституционному законодательству и государственному строительству по адресу www.Единыйурок.рф в разделе «Курсы».



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» (письмо Минобрнауки России от 14.05.2018 N 08-1184 «О направлении информации»)

https://dakad.ru/wp-content/uploads/Pismo_-Minobrnauki-Rossii-ot-14.05.2018-N-08-1184-O-napra.pdf

Разработаны 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.

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: информационные стенды, официальные интернет-ресурсы, средства массовой информации (школьные газеты, педагогические издания и другие).

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 № 1 к методическим рекомендациям представлен образец памятки для размещения на информационных стендах.

Формы и методы работы по развитию ресурсов устойчивости школьников различных возрастов к интернет-рискам и угрозам⁴



Выбор конкретных форм и методов работы с несовершеннолетними должен осуществляться в соответствии с их возрастными особенностями.

Универсальным методом изучения информированности несовершеннолетних об интернет-рисках и угрозах, средствах и способах защиты от них, а так же об отношении обучающихся к интернет-рискам и угрозам, к организуемой профилактической работе в условиях массовой образовательной организации является интернет-опрос (варианты опросников для обучающихся трех возрастных групп – 11-12, 13-14 и 15-16 лет, и методические рекомендации по его проведению разработаны ФГБНУ «Центр защиты прав и интересов детей» и размещены на сайте <http://www.fcprc.ru/>).

При изучении информированности родителей об интернет-рисках и угрозах, способах защиты от них может быть использован метод интернет-опроса или письменный опрос (примеры опросников размещены на сайте ФГБНУ «Центр защиты прав и интересов детей» <http://www.fcprc.ru/> и можно найти в публикациях, см., например, Солдатова Г.В., Зотова Е.Ю., Чекалина А.И., Гостимская О.С., 2011). В опросе могут принимать участие как все желающие родители, так и выборка родителей, скомплектованная педагогом-психологом с участием администрации образовательной организации.

Для информирования несовершеннолетних о средствах и способах защиты от интернет-рисков и угроз, о правилах работы в Сети, о ресурсах устойчивости к интернет-угрозам, способах их развития могут использоваться все информационные ресурсы образовательной организации: сообщения педагогов, оформление стендов, размещение советов, памяток, рекомендаций в классных уголках, рассылки с использованием электронных ресурсов и т.п.

Мероприятия профилактической направленности представлены в методических рекомендациях единых областных профилактических недель, приуроченных к календарным датам Российской Федерации в области профилактики социально-негативных явлений. Маршрутизаторы и методические рекомендации профилактических недель ежегодно обновляются специалистами ГКУ «Центр профилактики, реабилитации и коррекции».



Важным условием эффективности проводимых мероприятий является привлечение к их проведению представителей различных заинтересованных ведомств и организаций (учреждений здравоохранения, социальной

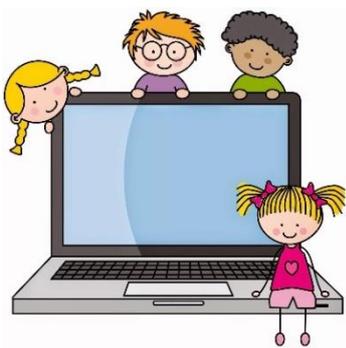
⁴ Калинина Н.В. С 23 Развитие устойчивости к интернет-рискам у детей и подростков. Методические рекомендации для педагогов. М.: ФГБНУ «Центр защиты прав и интересов детей», 2018. — 11 с.

защиты, силовых ведомств и др.).

В качестве совместных мероприятий могут выступать круглые столы и интернет-баттлы, открытые обсуждения и дискуссии. Важно, чтобы у школьников появилась возможность получить ответы на интересующие их вопросы из уст специалистов и получить доступ к получению индивидуальной консультации специалиста.

Развитие личностных качеств и социальных умений, выступающих ресурсами устойчивости несовершеннолетних к интернет-рискам и угрозам, может осуществляться на специальных занятиях с использованием методов активного социально-психологического обучения.

Детям младшего школьного возраста важно ознакомиться с общими правилами безопасного поведения в Интернете, узнать о существовании опасностей при работе в Интернете и способах защиты от них. Для них может быть проведена игра-путешествие в Интернет-пространство». Игра может быть проведена в отдельном классе или с участием всех классов начальной школы.

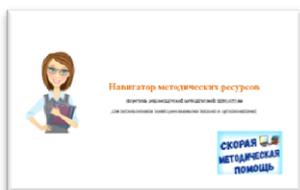


Для подростков актуальны тренинговые занятия, позволяющие выделить наиболее опасные угрозы и осознать имеющиеся ресурсы и способы защиты от них.



Вовлечение несовершеннолетних в совместную с педагогами и родителями профилактическую работу может осуществляться через организацию исследовательской деятельности обучающихся. Исследовательская деятельность сегодня является обязательной для обучающихся всех возрастов. Она организуется педагогами на уроках в рамках учебных предметов или во внеурочной деятельности. Исследовательская работа по изучению способов защиты от интернет-рисков и угроз может осуществляться в рамках программ внеурочных занятий (например, «Я – исследователь» в начальной школе), или через организацию работы школьных научных обществ, в рамках социального проектирования и т.п.

Материалы по формированию информационной безопасности детей, а также профессиональной информационной культуры педагогов, родителей предложены в Приложениях 3,4,5,6.



Деятельность образовательной организации по профилактике бесконтрольного использования личных мобильных устройств несовершеннолетних во время образовательного процесса

*В руках мобильный – мир в руках,
В кармане ли, так там и мир.
Без телефона только страх,
А с телефоном жизнь как пир.*
Шабалева Н.А.



В настоящее время мобильные устройства прочно вошли в нашу повседневную жизнь и оказались тесно переплетенными с работой, учебой и досугом. Особенно актуально это для детей и подростков, поскольку мобильный телефон с его постоянными уведомлениями, новостями, развлечениями и социальным взаимодействием оказывается мощным фактором воздействия на многие аспекты жизни ребенка, в том числе на его поведение и успеваемость.

Многочисленные исследования взаимосвязи между успеваемостью и использованием смартфона во время учебы — будь то урок в классе или выполнение домашнего задания — показывают, что такое взаимодействие может иметь ряд преимуществ. Однако, использование мобильных устройств в школах связывают и с негативными последствиями: отвлекаемость, снижение академических показателей, слабое усвоение материала. В связи с этим многие страны, включая и Россию, либо обсуждают введение ограничения на использование смартфонов в учебных заведениях, либо уже ввели их.

Действительно ли эта мера необходима, какова ее эффективность, на каком уровне должны приниматься подобные решения, какие профилактические мероприятия необходимо организовывать?

В данном разделе содержится обзор работ по этой проблеме, представлен международный опыт, а также рекомендации по профилактике бесконтрольного использования личных мобильных устройств несовершеннолетних в образовательных организациях Российской Федерации (в соответствии с действующим законодательством).

Исследование 2015 года, опубликованное в журнале «Компьютеры в человеческом поведении», издаваемом в Великобритании, продемонстрировало, что среди старшеклассников общее использование мобильных телефонов, измеряемое количеством минут в день и не ограниченное школьным временем, было «значительным и негативным предиктором академической успеваемости». В том же году Дакота Лоусон и Брюс Б. Хендерсон из Западно-Каролинского университета (США) провели исследование с целью изучить взаимосвязь между использованием мобильных телефонов в классе и пониманием учебной информации.

Выяснилось, что учащиеся, которые переписывались в классе, имели значительно более низкие результаты тестов, даже если представленный

материал был прост: использование мобильного телефона в классе ухудшает понимание и производительность учащихся. Эта работа была выполнена после нескольких аналогичных исследований в прошлом и подтвердила их результаты.

Исследователи Джулия Ирвин и Наташа Гупта из Университета Маккуори (Сидней) в 2016 году провели эксперимент, проверяя влияние отвлекающих факторов, связанных с Facebook, в классе. Исследователи обнаружили, что ученики, которые интересовались предметом и тем, как он был представлен, с меньшей вероятностью будут отвлекаться на Facebook. Тем не менее учащиеся, имевшие доступ к телефонам, работали хуже, чем те, кто его не имел. Несколько работ выявили отрицательную связь между использованием социальных сетей, таких как Facebook, MySpace или Twitter, и успеваемостью, причем такие результаты были обнаружены по всему миру, включая Северную Америку, Европу и Азию.

Коллективное исследование 2017 года, опубликованное в журнале «Прикладная когнитивная психология» («Applied Cognitive Psychology»), показало, что студенты колледжа запоминают меньше информации, когда им разрешают иметь с собой мобильный телефон во время лекций. В процессе эксперимента учащиеся, которым не был разрешен доступ к сотовому телефону, показали лучшие результаты.

Анализ международного опыта показал, что ранний возраст начала использования устройств мобильной связи и длительные накопленные время их использования являются факторами, ведущим к нарушениям психики, что проявляется у ребенка гиперактивностью, повышенной раздражительностью, снижением долговременной памяти и умственной работоспособности, нарушением коммуникативных способностей, расстройством сна.

Исследования, представленные в работах российских ученых, выявили негативные реакции у детей, использующих мобильные телефоны в образовательной организации, существенно отличающие их от сверстников, не использующих мобильные устройства. Негативные реакции проявлялись в виде ослабления смысловой памяти, снижения внимания, скорости аудиомоторной реакции, нарушений фонематического восприятия, раздражительности.

Проведенные исследования свидетельствуют об отрицательной зависимости времени пользования смартфоном и успеваемостью у обучающихся: чем больше времени ежедневно он тратит на смартфон, тем хуже справляется с учебным материалом.

Таким образом, интенсивное использование телефона даже для решения учебных задач может отрицательно сказываться на учебной деятельности. Объяснение полученной зависимости исследователи связывают с феноменом многозадачности.

Многофункциональность телефона, наличие множества приложений неизбежно создают ситуацию многозадачности, требующую постоянных переключений с одного вида активности на другой, в том числе в процессе

обучения. Это ведет к ухудшению усвоения материала и снижению успеваемости.



По мнению врачей, психологов существуют и более опасные последствия постоянного взаимодействия с телефоном:

номофобия – термин, являющийся аббревиатурой слов «фобия — без мобильного телефона» («no-mobile-phone phobia») страх остаться без телефона;

фоноголизм - когда использование телефона превращается в поведенческую зависимость, которую приходится контролировать.

Зависимость детей и подростков от телефона, планшета и иных гаджетов на сегодняшний день распространенное явление и таит в себе две группы опасностей:

✓ физические (к физическим опасностям зависимости от телефона у детей можно отнести непосредственное влияние гаджетов на растущий организм, как следствие существенное снижение физической активности, использование различного рода технологических решений трансформирует мысленные процессы и становится причиной расщепленности внимания, ухудшения памяти);

✓ социально-психологические (социально-психологическая опасность зависимости от телефона у детей кроется в сложности защиты от нежелательных контактов, использование социальных сетей и посещение сайтов с вредоносной информацией, при возникновении у подростков аддикции к мобильным телефонам формируется нарушенное представление об общении – подростки находятся в виртуальном мире и практически перестают нормально общаться в реальном).

Среди признаков зависимости от телефона и иных гаджетов стоит выделить: снижение способности концентрироваться; возникновение проблем с когнитивными способностями, среди которых – память; трудности, возникающие в процессе принятия решений; периодические головные боли, ухудшение зрения, боли в шейном отделе позвоночника; нарушения сна, бессонница; низкий уровень социализации. Помимо этого, подростки крайне болезненно переживают, если телефон оказывается не рядом, нервничают, не представляют жизни без него. Крайне часто дети, имеющие аддикцию к мобильным телефонам, проверяют сообщения, заходят в социальные сети, плохо себя чувствуют, если телефоном невозможно воспользоваться или он разрядился.



Игнорирование признаков зависимости от телефона и иных гаджетов может стать причиной ухудшения здоровья и привести к цифровой деменции, что подразумевает расстройство памяти.

Опыт других стран⁵

На основе открытых источников: правительственных сайтов, публикаций в прессе, справочной литературы — проведен анализ ограничительных мер в отношении мобильных устройств в учебных заведениях разных стран.



СТРАНА: Великобритания, год запрета – 2007 год.

КАК ВЫГЛЯДИТ ЗАПРЕТ: либо нельзя вообще приносить смартфон в школу, либо он сдается в начале дня в специальный ящик для хранения. Учащиеся, которых ловят с мобильными телефонами в учебные часы, могут получить взыскание. Возможности использования смартфона определяются уставом каждой конкретной школы.

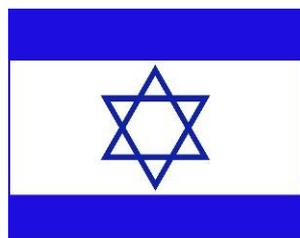
ПОСЛЕДСТВИЯ И КОММЕНТАРИИ: согласно исследованию, проведенному Лондонской школой экономики, успеваемость учащихся улучшилась, когда были введены установления, запрещающие использование сотовых телефонов в школах. Этот запрет не только помог учащимся получить более высокий балл на экзаменах, но и снял такую проблему, как соблазн использовать сотовые телефоны не для учебы. Однако школы заметили, что положительное влияние запрета больше касалось учеников в возрасте до одиннадцати лет. Учащиеся старшего возраста страдали от ограниченного использования на своих телефонах образовательных приложений, помогающих в обучении или приобретении навыков.

СТРАНА: Франция, год запрета - 2018 год.

КАК ВЫГЛЯДИТ ЗАПРЕТ: запрещено использовать смартфоны во всех начальных и средних школах в течение всего дня, в том числе в перерывах, за исключением случаев крайней необходимости. Ученикам предлагается убрать свои мобильные телефоны или положить их в шкафчик. Закон позволяет учителям конфисковать телефоны до конца дня в случаях несоблюдения запрета.



ПОСЛЕДСТВИЯ И КОММЕНТАРИИ: запрет продолжает активно обсуждаться и постепенно начинает действовать в разных школах, поскольку не везде есть возможность обеспечить места для хранения смартфонов в течение учебного дня.



СТРАНА: Израиль, год запрета - 2016 год.

КАК ВЫГЛЯДИТ ЗАПРЕТ: запрещено пользоваться смартфонами во время учебы и приносить их на занятия. В 2017 году министерство образования запретило личное использование мобильных телефонов не только для студентов, но и для преподавателей. Запрет действует только в часы обучения.

⁵ Электронный журнал «Дети в информационном обществе» ГАДЖЕТЫ И ЗДОРОВЬЕ: МИФЫ, ФАКТЫ, ДИСКУССИИ №31, 2019г.



СТРАНА: Япония, год запрета - 2009 год.

КАК ВЫГЛЯДИТ ЗАПРЕТ: Решения об использовании смарт-фонов и других цифровых устройств принимаются в каждой школе самостоятельно.

ПОСЛЕДСТВИЯ И КОММЕНТАРИИ: в настоящее время все большее число школ разрешают использовать мобильные телефоны в качестве учебного пособия. Спустя 10 лет после введения запрета министерство образования и науки пришло к выводу, что он уже не соответствует времени и не является актуальным в условиях современной образовательной среды.

Россия: мнения школьников и их родителей

По итогам опроса ⁶ общественного мнения (проведённого Минпросвещением России, Рособрнадзором и Роспотребнадзором) 61% учащихся, 89% родителей и 90% педагогов поддержали ограничение использования мобильных телефонов школьниками во время уроков. Около трёх четвертей опрошенных считают, что и педагоги должны ограничить использование сотового телефона в школе в присутствии обучающихся в личных целях. Более половины школьников согласны с тем, что неупорядоченное использование мобильных телефонов может нанести вред их здоровью и отвлекает от учебного процесса. Среди взрослых участников опроса (родителей и педагогов) с этими утверждениями согласны 83–90% опрошенных.



На сегодняшний день в Российской Федерации не существует закона, запрещающего использование мобильных средств в образовательной организации.

2019 год стал одним из важных в системе образования. В августе 2019 года Роспотребнадзор, Минпросвещения, Рособрнадзор и Российская академия образования подготовили методические рекомендации о порядке использования личных устройств мобильной связи («Методические рекомендации об использовании устройств мобильной связи в общеобразовательных организациях» (утв. Роспотребнадзором N МР 2.4.0150-19, Рособрнадзором N 01-230/13-01 14.08.2019) вместе с «Результатами исследований, показавших отрицательные последствия использования устройств мобильной связи на здоровье детей», «Памяткой для обучающихся, родителей и педагогических работников по профилактике неблагоприятных для здоровья и обучения детей эффектов от воздействия устройств мобильной связи») познакомится подробно с данным документом



⁶ Методические рекомендации об использовании устройств мобильной связи в общеобразовательных организациях» (утв. Роспотребнадзором N МР 2.4.0150-19, Рособрнадзором N 01-230/13-01 14.08.2019)

можно на сайте Роспотребнадзора (https://rospotrebnadzor.ru/upload/iblock/bb7/mr-telefony-v-obrazovatelnykh-org-_1_.pdf).

В представленном документе органам управления образованием субъектов Российской Федерации, местного самоуправления в сфере образования и общеобразовательным организациям с целью профилактики возможного вреда здоровью школьников и повышения эффективности образовательного процесса рекомендуется рассмотреть вопрос об ограничении использования мобильных устройств связи в образовательных организациях обучающимися, за исключением детей, нуждающихся в пользовании такими устройствами по состоянию здоровья (мониторинг сахара крови при сахарном диабете 1 типа и др.), а также педагогическими работниками и родителями в целях снижения рисков нанесения вреда здоровью и развитию детей в связи с использованием устройств мобильной связи.

В частности, рекомендуется предусмотреть для всех участников образовательного процесса целесообразность перевода устройств мобильной связи в режим «без звука» при входе в образовательную организацию, а также ограничить использование школьниками устройств мобильной связи во время учебного процесса.

При необходимости и возможности школам рекомендуется предусмотреть места хранения мобильных телефонов учеников во время образовательного процесса, согласовать способы коммуникации родителей с обучающимися в случае возникновения необходимости или внештатной ситуации.

Профилактика бесконтрольного использования устройств мобильной связи в образовательных организациях

В результате полученных данных можно было бы вообще запретить использование мобильных телефонов и смартфонов в классе, школе. Однако важно понимать, что телефон, смартфон, как и любая другая технология, всего лишь инструмент. Пользу он принесёт или вред – во многом зависит от эффективно организованной профилактической работы. Современных детей будут постоянно окружать сверстники с гаджетами. Лишение подростка возможности использования гаджета без альтернативной замены – вызов (особенно если речь идёт о зависимом поведении).

Если рассматривать ситуацию с этой стороны, становится очевидным, что политика тотального запрета на гаджеты в учебных заведениях выглядит слишком экстремальной и необоснованной. Для эффективного интегрирования технологий в учебные классы и снижения восприимчивости учеников к «помехам» педагогам рекомендуется:

1. Проводить мероприятия, направленные на воспитание культуры использования устройств мобильной связи у всех участников образовательного процесса, с использованием воспитательного потенциала

совместной работы (педагогического коллектива с детьми, старшеклассников с младшими детьми) в части воспитания культуры использования устройств мобильной связи. *Создавать ресурсы, которые помогут конструировать увлекательные, информативные, интерактивные занятия, способные превзойти привлекательность социальных сетей (цифровые устройства способствуют положительным результатам обучения, когда они включены в образовательную среду, используются для веб-исследований, онлайн-тестирований, поиска дополнительной информации по теме, для проведения викторин и марафонов в игровом формате). Учителя, к примеру, могут использовать кликеры — приложения и личные устройства, которые позволяют им задавать вопросы ученикам и сразу же собирать, и просматривать ответы всего класса. Эта интерактивная технология не только простимулирует внимание учащихся к материалу курса, но также предотвратит посещение «посторонних» ресурсов. Другой пример стратегии обучения с использованием мобильных устройств — попросить учеников найти в интернете недостающую информацию по теме урока или лекции, найти интересный веб-сайт или онлайн-видео, чтобы поделиться с классом. Создавать, развивать сайты и (или) страницы сайтов педагогических работников в сети «Интернет» (Методические рекомендации по созданию и развитию сайтов и (или) страниц сайтов педагогических работников в сети «Интернет», подготовлены Временной комиссией Совета Федерации по развитию информационного общества <https://ддтанива.pdf/wp-content/uploads/2020/05/Методические-рекомендации-по-созданию-и-развитию-сайтов-и-страниц-сайтов-педагогических-работников.pdf>). Организовывать работу клубов общения, в процессе клубных встреч у детей будет обеспечиваться формирование позитивной самооценки, снижение эмоционального напряжения, развитие чувства доверия к себе и окружающим, повышение уверенности в себе, развитие навыков конструктивного взаимодействия и реального общения со сверстниками.*

2. Проводить разъяснительную работу с родителями и обучающимися по вопросам профилактики неблагоприятных для здоровья и обучения детей эффектов от воздействия устройств мобильной связи и воспитания культуры пользования такими устройствами (приложение №6).

3. Обеспечить психолого-педагогическое сопровождение процесса, связанного с ограничением использования устройств мобильной связи в образовательной организации. Для определения мобильной зависимости использовать диагностические методики, анкеты (методика для определения потребности в общении; методика определения ситуативной и личностной тревожности Ч. Спилбергера-Ю. Ханина; шкала одиночества Д. Рассела, Л. Пепло, М. Фергюсона, выбор данных методик обоснован их надежностью и валидностью, а также тем, что они позволяют диагностировать основные важные стороны психологического состояния

подростков – потребность в общении, тревожность, чувство одиночества, «симптомы» аддиктивного поведения.

4. Использовать время перемен для общения, активного отдыха обучающихся между уроками (занятиями), восполнения их физиологической потребности в двигательной активности с учетом возрастных норм (*Методические рекомендации «Фитнес как профилактика стрессов у обучающихся образовательных организаций» ГКУ «Центр профилактики, реабилитации и коррекции», 2022 год*); при необходимости - использование на переменах устройств мобильной связи по прямому назначению (для звонка, смс-сообщения).

5. Осуществлять мониторинг и анализ работы образовательных организаций по упорядочению использования участниками образовательных отношений устройств мобильной связи с целью профилактики неблагоприятного воздействия на здоровье и обучение детей, а также повышения эффективности образовательного процесса.

Ограничения использования мобильных устройств связи обучающимися в образовательных организациях должны быть закреплены в локальных актах: уставе, положениях, приказах.

Заключение

Безопасная школа, социальное окружение — необходимые условия нормального развития ребенка. Они обеспечиваются целой системой мер и действий: созданием доброжелательной и принимающей атмосферы в школе; разработкой алгоритмов действия; подготовкой материально технического обеспечения для эффективной работы; взаимодействием с соответствующими службами муниципального, регионального и федерального уровней. Эти и другие шаги составляют основу системы, обеспечивающей психологическую и информационную безопасность образовательной среды. Её специфика определяет как трудности, так и дополнительные возможности такой системы.

Взаимодействие всех субъектов профилактики в разработке и реализации мер профилактики Интернет-рисков позволяет реализовать стратегические задачи профилактики: дает возможность управлять этими рисками, а так же позволяет наращивать ресурсы стойкости к негативному воздействию Интернета у всех участников за счет повышения их информированности о возможных рисках, осознания механизмов негативного воздействия на пользователей, взаимообогащения участников способами и средствами противодействия Интернет-рискам.

К участию в совместной профилактической работе могут активно привлекаться сотрудники ППМС-центров, комиссий по делам несовершеннолетних и защите их прав, силовых структур, медицинских организаций, общественных организаций и других заинтересованных ведомств.

Литература

1. Бояров, Е.Н. Ключевые проблемы информационной безопасности сферы образования [Электронный ресурс] / Е.Н. Бояров. – URL: <https://moluch.ru/th/3/archive/43/1500/> (дата обращения: 02.11.2020).
2. Безопасность детей в интернете [Электронный ресурс]. –URL: <http://www.ifar.ru/library/book099.pdf> (дата обращения: 11.02.2022).
3. Галутва Н. В. Использование гаджетов школьниками — польза или вред? // Ямальский вестник.-2019.-№ 4. — С. 40–45. Карпухова М. И. Использование гаджетов современными российскими школьниками как педагогическая проблема // Молодёжь и наука: актуальные проблемы педагогики и психологии.-2018.-№ 3. — С. 43–47.
4. Габер И.В., Зарецкий В.В., Артамонова Е.Г., Ефимова О.И., Калинина Н.В. Обеспечение психологической безопасности образовательной среды. Методические рекомендации для руководителей общеобразовательных организаций.: — М.: ФГБНУ «Центр защиты прав и интересов детей», 2018. — 60 с.
5. Дубов, С.С. Информационная безопасность ребенка в цифровом пространстве Российской Федерации [Электронный ресурс] / С.С. Дубов, В.В.Линьков, М.А.Карбаинова. –URL: https://rtj.mirea.ru/upload/medialibrary/27c/RTZH_2019_4_21_30.pdf (дата обращения: 04.02.2022).
6. Дети России онлайн [Электронный ресурс]. –URL: <https://ediniy-urok.ru/urok-bezopasnosti-v-sinternet/http://detionline.com/helpline/rules/parents> (дата обращения: 11.02.2022).
7. Кондратьева, Е.С. Развитие познавательного интереса у младших школьников через использование информационных технологий на уроках математики / Е.С. Кондратьева // Проблемы педагогики. – 2015. – №1(2). – С. 34-39.
8. Кондратьева, Е.С. Развитие познавательного интереса у младших школьников через использование информационных технологий на уроках математики / Е.С. Кондратьева // Проблемы педагогики. – 2015. – №1(2). – С. 34-39.
9. Лавриненко А. И. Запрет на использование гаджетов в школе: за и против / А. И. Лавриненко. — Текст: непосредственный // Молодой ученый. — 2020. — № 15 (305). — С. 54-57. [Электронный ресурс]. — URL: <https://moluch.ru/archive/305/68786/> (дата обращения: 11.02.2022).
10. Молодцова, Е.Ю. К вопросу организации мероприятий по информационной безопасности учащихся в образовательном учреждении / Е.Ю. Молодцова, М.Ю. Склямина [Электронный ресурс] / Е.Ю. Молодцова. – URL: <https://moluch.ru/archive/77/13215/> (дата обращения: 02.02.2022).
11. Методические рекомендации об использовании устройств мобильной связи в общеобразовательных организациях [Электронный ресурс] // Роспотребнадзор РФ. URL:

https://rospotrebnadzor.ru/upload/iblock/bb7/mr-telefony-v-obrazovatelnykh-org-_1_.pdf (дата обращения 25.01.2022)

12. Поливанова К. Н., Королева Д. О. Социальные сети как новая практика развития городских подростков. // Вестник Российского фонда фундаментальных исследований. Гуманитарные и общественные науки. - 2016.-№ 1. — С. 173–182.

13. Российская школа и новые информационные технологии: взгляд в следующее десятилетие. – М.: Изд-во «НексПринт», 2010. – 95 с.

ПРИЛОЖЕНИЯ

Приложение 1.

Нормативно-правовое обеспечение информационной безопасности образовательной среды

Федеральные законы РФ

1. Федеральный закон от 24.07.1998 № 124-ФЗ «Об основных гарантиях прав ребенка в Российской Федерации».
2. Федеральный закон Российской Федерации от 29 декабря 2012 г. № 273-ФЗ «Об образовании в Российской Федерации».
3. Федеральный закон от 29.12.2010 № 436-ФЗ «О защите детей от информации, причиняющей вред их здоровью и развитию».
4. Федеральный закон от 13.03.2006 № 38-ФЗ «О рекламе».
5. Федеральный закон от 27.07.2006 № 149-ФЗ «Об информации, информационных технологиях и о защите информации».
6. Федеральный закон от 27.07.2006 № 152-ФЗ «О персональных данных».
7. Федеральный закон от 28.12.2010 № 390-ФЗ «О безопасности».
8. Федеральный закон Российской Федерации от 23 июня 2016 г. № 182-ФЗ «Об основах системы профилактики правонарушений в Российской Федерации».

Указы Президента РФ Указ Президента

1. Указ Президента РФ от 31.12.2015 № 683 «О Стратегии национальной безопасности Российской Федерации».
2. Указ Президента РФ от 05.12.2016 № 646 «Об утверждении Доктрины информационной безопасности Российской Федерации».

Постановления и распоряжения Правительства РФ

3. Концепция информационной безопасности детей. Утверждена распоряжением Правительства Российской Федерации от 2 декабря 2015 г. №2471-р.
4. Постановление Правительства РФ от 1 ноября 2012 г. N 1119 «Об утверждении требований к защите персональных данных при их обработке в информационных системах персональных данных».
5. Постановление Правительства РФ от 21 марта 2012 г. N 211 «Об утверждении перечня мер, направленных на обеспечение выполнения обязанностей, предусмотренных Федеральным законом «О персональных данных» и принятыми в соответствии с ним нормативными правовыми актами, операторами, являющимися государственными или муниципальными органами».
6. СанПиН 2.4.2.2821-10 «Санитарно-эпидемиологические требования к условиям и организации обучения общеобразовательных учреждениях».

Ведомственные и инструктивные документы

1. Приказ Минкомсвязи России от 10 апреля 2013 г. № 81 «Об утверждении Административного регламента исполнения Федеральной службой по надзору в сфере связи, информационных технологий и массовых коммуникаций государственной функции по осуществлению государственного контроля и надзора за соблюдением законодательства Российской Федерации о защите детей от информации, причиняющей вред их здоровью и (или) развитию».

2. Письмо Минобрнауки России от 28 апреля 2014 г. № ДЛ-115/03 «О направлении методических материалов для обеспечения информационной безопасности детей при использовании ресурсов сети Интернет» (вместе с «Методическими рекомендациями по ограничению в образовательных организациях доступа обучающихся к видам информации, распространяемой посредством сети «Интернет», причиняющей вред здоровью и (или) развитию детей, а также не соответствующей задачам образования», «Рекомендациями по организации системы ограничения в образовательных организациях доступа обучающихся к видам информации, распространяемой посредством сети Интернет, причиняющей вред здоровью и (или) развитию детей, а также не соответствующей задачам образования»).

3. Письмо Минобрнауки России от 19 декабря 2017 г. № 07-7453 «О направлении методических рекомендаций по стимулированию вовлечения детей, состоящих на различных видах учета, в общественно значимые мероприятия, в том числе в добровольческую и волонтерскую деятельность».

4. Приказ Минкомсвязи России от 16 июня 2014 г. № 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».

5. Методические рекомендации по созданию и развитию сайтов и (или) страниц сайтов педагогических работников в сети «Интернет», подготовлены Временной комиссией Совета Федерации по развитию информационного общества, 2017г.

6. Письмо департамента государственной политики в сфере оценки качества общего образования, Минпросвещения России № 04-474 от 07.06.2019 «О методических рекомендациях» (вместе с Методическими рекомендациями по ограничению в образовательных организациях доступа обучающихся к видам информации, распространяемой посредством сети «Интернет», причиняющей вред здоровью и (или) развитию детей, а также не соответствующей задачам образования.)

7. Письмо Минкомсвязи России от 30.05.2019 № АВ-П17-062-11826 «О методических рекомендациях» (вместе с Методическими рекомендациями по основам информационной безопасности детей, находящихся в организациях отдыха детей и их оздоровления).

8. Письмо Департамента государственной политики в сфере общего образования Минпросвещения РФ № 03-39 от 29.03.2019 г. «О методических

рекомендациях» (вместе с Методические рекомендации по реализации мер, направленных на обеспечение безопасности и развития детей в сети «Интернет»).

9. Письмо члена Совета Федерации Российской Федерации Боковой Л.Н.№66-02.41/ЛБ от 26.02.2019 г. Материалы в разделе «Проекты» сайта Единый урок. Методические рекомендации по ограничению в образовательных организациях доступа обучающихся к видам информации, распространяемой посредством сети «Интернет», причиняющей вред здоровью и (или) развитию детей, а также не соответствующей задачам образования.

Образцы локальных актов образовательной организации в области
информационной безопасности детей.⁷

П Р И К А З

20... .. г.

№ _____

г. _____

**Об организации информационной безопасности
в образовательной организации**

В целях осуществления ограничения доступа обучающихся к видам информации, распространяемой посредством сети "Интернет", причиняющей вред здоровью и (или) развитию детей, а также не соответствующей задачам образования, приказываю:

1. Утвердить:

- Журнал учета доступа в сеть Интернет;
- График работы точки доступа к сети Интернет;
- Примерный акт установки системы контентной фильтрации в образовательном учреждении;
- Журнал регистрации случаев обнаружения сайтов;
- Положение об ограничении доступа обучающихся к видам информации, распространяемой посредством сети «Интернет», причиняющей вред здоровью и (или) развитию детей, а также не соответствующей задачам образования;
- Журнал контроля контентной фильтрации;
- План мероприятий по обеспечению информационной безопасности обучающихся на 2019-2022 годы;
- Акт проверки контентной фильтрации в образовательной организации;
- Должностная инструкция лица, ответственного за организацию доступа к сети Интернет и внедрение системы контентной фильтрации в образовательном учреждении;
- Формулировки для внесения изменений в должностные инструкции педагогических работников и иных работников образовательной организации об ограничении доступа обучающихся к видам информации, распространяемой посредством сети «Интернет», причиняющей вред здоровью и (или) развитию детей, а также не соответствующей задачам образования.

2. Назначить ответственными за организацию доступа к сети Интернет в _____ следующих работников:

- В кабинете информатики - учителя информатики _____
- В учебных кабинетах, имеющих точку доступа к сети Интернет - учителей – предметников
- В библиотеке – библиотекаря _____.

3. Системному администратору/Учителю информатики/Программисту:

- установить аппаратное или программное обеспечение, осуществляющее контент-фильтрацию ресурсов сети Интернет на основе Реестра безопасных образовательных сайтов Перечень.

⁷ Опубликованы на сайте Экспертного совета по информатизации системы образования и воспитания при Временной комиссии Совета Федерации (соответствуют - Методическим рекомендациям по ограничению в образовательных организациях доступа обучающихся к видам информации, распространяемой посредством сети «Интернет», причиняющей вред здоровью и (или) развитию детей, а также не соответствующей задачам образования, разработанным Экспертным советом, дата подписания Минкомсвязи РФ 16 мая 2019 г.)

- обеспечить контроль работы контентной-фильтрации _____ на постоянной основе.
 - еженедельно проверять точки доступа к сети Интернет _____ на предмет выявления обращений к ресурсам, содержащим информацию, причиняющей вред здоровью и (или) развитию детей, а также не соответствующей задачам образования;
 - при обнаружении обращений ресурсам, н содержащим информацию, причиняющей вред здоровью и (или) развитию детей, а также не соответствующей задачам образования, немедленно сообщать директору _____ целью своевременного принятия незамедлительных мер к исключению доступа к подобной информации.
4. Специалисту по кадровой работе _____ ознакомить сотрудников образовательного учреждения с данным приказом и его приложениями, срок — исполнения до _____.
5. Контроль за выполнением приказа оставляю за собой.

Директор _____ / _____
(подпись) (Ф.И.О.)

" ____ " _____ 20__ г.

Положение об ограничении доступа обучающихся к видам информации, распространяемой посредством сети «Интернет», причиняющей вред здоровью и (или) развитию детей, а также не соответствующей задачам образования

Общие положения

1. Использование сети Интернет в _____ (далее ОУ) направлено на решение задач учебно-воспитательного процесса.
2. Настоящее Положение регулирует условия и порядок использования сети Интернет в ОУ.
3. Настоящее Положение имеет статус локального нормативного акта ОУ.
4. Настоящее Положение разработано в соответствии с требованиями Методических рекомендации по ограничению в образовательных организациях доступа обучающихся к видам информации, распространяемой посредством сети "Интернет", причиняющей вред здоровью и (или) развитию детей, а также не соответствующей задачам образования.

Организация использования сети Интернет в ОУ

1. Вопросы использования возможностей сети Интернет в учебно-образовательном процессе рассматриваются на педагогическом совете ОУ. Педагогический совет утверждает Правила использования сети Интернет на учебный год. Правила вводятся в действие приказом руководителя ОУ.
2. Правила использования сети Интернет разрабатывается педагогическим советом ОУ на основе примерного регламента самостоятельно либо с привлечением внешних экспертов, в качестве которых могут выступать:
 - преподаватели других образовательных учреждений, имеющие опыт использования Интернета в образовательном процессе;
 - специалисты в области информационных технологий;
 - представители органов управления образованием.
3. При разработке правил использования сети Интернет педагогический совет руководствуется:
 - законодательством Российской Федерации;
 - опытом целесообразной и эффективной организации учебного процесса с использованием информационных технологий и возможностей Интернета;
 - интересами обучающихся;
 - целями образовательного процесса;
 - методическими рекомендациями по ограничению в образовательных учреждениях доступа обучающихся к видам информации, распространяемой посредством сети "Интернет", причиняющей вред здоровью и (или) развитию детей, а также не соответствующей задачам образования.
4. Руководитель ОУ отвечает за обеспечение эффективного и безопасного доступа к сети Интернет в ОУ, а также за выполнение установленных правил. Для обеспечения доступа участников образовательного процесса к сети Интернет в соответствии с установленным в ОУ правилами руководитель ОУ назначает своим приказом ответственного за организацию работы с Интернетом и ограничение доступа.
5. Педагогический совет ОУ:
 - принимает решение о разрешении/блокировании доступа к определенным ресурсам и (или) категориям ресурсов сети Интернет;
 - определяет характер и объем информации, публикуемой на Интернет-ресурсах ОУ;
 - дает руководителю ОУ рекомендации о назначении и освобождении от исполнения своих функций лиц, ответственных за обеспечение доступа к ресурсам сети Интернет и контроль безопасности работы в Сети;

6. Во время уроков и других занятий в рамках учебного плана контроль использования обучающимися сети Интернет осуществляет преподаватель, ведущий занятие. При этом преподаватель:
 - наблюдает за использованием компьютера и сети Интернет обучающимися;
 - принимает меры по пресечению обращений к ресурсам, содержащие информацию, причиняющей вред здоровью и (или) развитию детей, а также не соответствующей задачам образования.
7. Во время свободного доступа обучающихся к сети Интернет вне учебных занятий, контроль использования ресурсов Интернета осуществляют работники ОУ, определенные приказом его руководителя.
8. Работник образовательного учреждения:
 - наблюдает за использованием компьютера и сети Интернет обучающимися;
 - принимает меры по пресечению по пресечению обращений к ресурсам, содержащие информацию, причиняющей вред здоровью и (или) развитию детей, а также не соответствующей задачам образования;
 - сообщает классному руководителю о преднамеренных попытках обучающегося осуществить обращение к ресурсам, содержащие информацию, причиняющей вред здоровью и (или) развитию детей, а также не соответствующей задачам образования.
9. При использовании сети Интернет в ОУ обучающимся предоставляется доступ только к сайтам, включенным в Реестр безопасных образовательных сайтов. Проверка выполнения такого требования осуществляется с помощью специальных технических средств и программного обеспечения контентной фильтрации, установленного в ОУ или предоставленного оператором услуг связи.
10. Отнесение определенных ресурсов и (или) категорий ресурсов в соответствующие группы, доступ к которым регулируется техническим средствами и программным обеспечением контентной фильтрации, в соответствии с принятыми в ОУ правилами обеспечивается работником ОУ, назначенным его руководителем.

3. Использование сети Интернет в образовательном учреждении

1. В ОУ используются только сайты в сети «Интернет», включенные в Реестр безопасных образовательных сайтов. Использование сайтов в сети «Интернет», не включенных в Реестр безопасных образовательных сайтов, запрещается.
2. Контроль за использованием обучающимися сети Интернет осуществляют:
 - во время занятия — проводящий его учитель и (или) сотрудник ОУ, специально выделенный для помощи в проведении занятий;
 - во время использования сети Интернет для свободной работы обучающихся — сотрудник ОУ, назначенный руководителем ОУ в установленном порядке.
3. Лицо, осуществляющее контроль за использованием обучающимися сети Интернет:
 - определяет время и место работы обучающихся в сети Интернет с учетом использования в образовательном процессе соответствующих технических возможностей, а также длительность сеанса работы каждого обучающегося;
 - наблюдает за использованием обучающимися компьютеров и сети Интернет;
 - способствует осуществлению контроля объемов трафика ОУ в сети Интернет;
 - запрещает дальнейшую работу обучающегося в сети Интернет на уроке (занятии) в случае нарушения им порядка использования сети Интернет и предъявляемых к обучающимся требований при работе в сети Интернет;
 - доводит до классного руководителя информацию о нарушении обучающимся правил работы в сети Интернет;
 - принимает необходимые меры по пресечению обращений к ресурсам, не имеющим отношения к образовательному процессу.
4. Обучающемуся запрещается:
 - обращаться к ресурсам, содержание и тематика которых не допустимы для несовершеннолетних и/или нарушают требованиям, установленным для сайтов Реестра безопасных образовательных сайтов;

- осуществлять любые сделки через Интернет;
 - осуществлять загрузки файлов на компьютер ОУ без специального разрешения.
5. При обнаружении ресурса, содержащего информацию, причиняющей вред здоровью и (или) развитию детей, а также не соответствующей задачам образования, обучающийся обязан незамедлительно сообщить об этом преподавателю, проводящему занятие. Преподаватель, в том числе самостоятельно выявивший ресурс, содержащий информацию, причиняющей вред здоровью и (или) развитию детей, а также не соответствующей задачам образования, обязан зафиксировать доменный адрес ресурса и время его обнаружения и сообщить об этом лицу, ответственному за работу локальной сети и ограничение доступа к информационным ресурсам.
6. Ответственный обязан:
- принять информацию от преподавателя;
 - направить информацию о выявлении ресурса оператору Реестра безопасных образовательных сайтов в течение суток;
 - в случае явного нарушения обнаруженным ресурсом законодательства Российской Федерации сообщить о нем по специальной "горячей линии" для принятия мер в соответствии с законодательством Российской Федерации.
7. Передаваемая информация должна содержать:
- доменный адрес ресурса;
 - сообщение о тематике ресурса;
 - дату и время обнаружения;
 - информацию об установленных в ОУ технических средствах технического ограничения доступа к информации.
8. В случае отказа доступа к ресурсу, разрешенному в ОУ, преподаватель также сообщает об этом лицу, ответственному за работу Интернета и ограничение доступа.

Принято:
Педагогическим советом
от «__» _____ 2019 г.

Утверждаю:

Директор

от «__» ____ 2019 г.

План мероприятий по обеспечению информационной безопасности обучающихся на 2019-2022 годы

№	Мероприятие	Сроки
1.	Изучение нормативно- правовой базы, методических рекомендаций и издание (актуализация) организационно-распорядительных документов по вопросам обеспечения информационной безопасности обучающихся при организации доступа к сети Интернет	Июнь - август
2.	Заключение договора с оператором связи на оказание услуг доступа к сети Интернет с контентной фильтрацией	Декабрь - январь
3.	Настройка (установка) технических средств, применяемых при организации доступа к сети Интернет (компьютерное оборудование, сетевое оборудование, системное и прикладное программное обеспечение) в соответствии с требованиями методических рекомендаций по ограничению в образовательных организациях доступа обучающихся к видам информации, распространяемой посредством сети "Интернет", причиняющей вред здоровью и (или) развитию детей, а также не соответствующей задачам образования,	Июнь - август
4.	Установка, конфигурация, настройка режимов работы технических средств контентной фильтрации	Июнь - август
5.	Ознакомление работников образовательной организации с методическими рекомендациями по ограничению в образовательных учреждениях доступа обучающихся к видам информации, распространяемой посредством сети "Интернет", причиняющей вред здоровью и (или) развитию детей, а также не соответствующей задачам образования, и локальных нормативных актов образовательной организации по вопросам обеспечения информационной безопасности обучающихся при организации доступа к сети Интернет	Август
6.	Ознакомление работников образовательной организации с сайтами в сети «Интернет», включенных в Реестр безопасных образовательных сайтов	Август

7.	Информирование работников образовательной организации, обучающихся и их родителей (законных представителей) об ответственности за нарушение требований законодательства Российской Федерации и организационно-распорядительных документов образовательной организации по вопросам обеспечения информационной безопасности обучающихся при организации доступа к сети Интернет	Август - сентябрь
8.	Информирование родителей (законных представителей) обучающихся о существующих угрозах в сети Интернет, о методах и способах защиты детей от информации, причиняющей вред здоровью и (или) развитию детей	Сентябрь- октябрь
9.	Проведение периодического контроля состояния системы обеспечения информационной безопасности обучающихся при организации доступа к сети Интернет	Не менее 3-ех в течении учебного года
10.	Организация преподавания обучающимся основ информационной безопасности в рамках реализации образовательной программы образовательной организации <i>В соответствии методическими рекомендациями по основам информационной безопасности для обучающихся общеобразовательных организаций с учётом информационных, потребительских, технических и коммуникативных аспектов информационной безопасности</i>	В течении учебного года
11.	Проведение Единого урока по безопасности в сети «Интернет»	Октябрь
12.	Проведение серии мероприятий проекта «Сетевичок» для обучающихся	Октябрь- ноябрь
13.	Организация участия педагогических работников в дистанционной конференции по формированию детского информационного пространства «Сетевичок»	Октябрь- ноябрь
14.	Проведение Всероссийской контрольной работы по информационной безопасности <i>На сайте www.Единыйурок.дети</i>	Октябрь- ноябрь
15.	Ведение локальных нормативных актов образовательной организации в области информационной безопасности обучающихся	В течении учебного года
16.	Оформление и обновление стенда «Информационная безопасность» <i>В соответствии с письмом Минобрнауки России от 14.05.2018 N 08-1184 «О направлении информации»</i>	В течении учебного года
17.	Размещение на официальном сайте образовательной организации информации по вопросам обеспечения информационной безопасности детей	В течении учебного года

	<i>В соответствии с письмом Минобрнауки России от 14.05.2018 N 08-1184 «О направлении информации»</i>	
18.	Прохождения педагогическими и иными работниками образовательной организации программы повышения квалификации на сайте Единыйурок.рф по направлению «Безопасное использование сайтов в сети «Интернет» в образовательном процессе в целях обучения и воспитания обучающихся в образовательной организации».	Раз в два календарных года
19.	Участие сотрудников образовательной организации в работе Экспертного совета по информатизации системы образования и воспитания при Временной комиссии Совета Федерации по развитию информационного общества в сфере образования и воспитания.	В течении учебного года
20.	Участие обучающихся, родителей (законных представителей) обучающихся и сотрудников образовательной организации в деятельности Межрегионального детского движения в области обеспечения безопасности и развития детей в информационном пространстве «Страна молодых»	В течении учебного года
21.	Использование в работе образовательных программ, направленных на формирование навыков у обучающихся, их родителей и педагогических работников безопасного поведения в информационной среде, рекомендованных Экспертным советом по информатизации системы образования и воспитания при Временной комиссии Совета Федерации по развитию информационного общества	В течении учебного года

Формулировки для внесения изменений в должностные инструкции педагогических работников и иных работников образовательной организации об ограничении доступа обучающихся к видам информации, распространяемой посредством сети «Интернет», причиняющей вред здоровью и (или) развитию детей, а также не соответствующей задачам образования

Должностная инструкция лица, ответственного за организацию доступа к сети Интернет и внедрение системы контентной фильтрации в образовательном учреждении

1. Общие положения

Должен знать:

- дидактические возможности использования ресурсов сети Интернет;
- правила безопасного использования сети Интернет;
- методические рекомендации по ограничению в образовательных организациях доступа обучающихся к видам информации, распространяемой посредством сети "Интернет", причиняющей вред здоровью и (или) развитию детей, а также не соответствующей задачам образования.

2. Должностные обязанности:

- планирует использование ресурсов сети Интернет в образовательном учреждении на основании заявок преподавателей и других работников образовательного учреждения;
- разрабатывает, согласует с педагогическим коллективом, представляет на педагогическом совете образовательного учреждения локальные нормативные акты образовательной организации в сфере обеспечения информационной безопасности детей;
- организует получение сотрудниками образовательного учреждения электронных адресов и паролей для работы в сети Интернет и информационной среде образовательного учреждения;
- организует контроль использования сети Интернет в образовательном учреждении;
- организует контроль работы оборудования и программных средств, обеспечивающих использование Реестра безопасных образовательных сайтов в образовательной организации;
- организует контроль реализации в образовательном учреждении методических рекомендации по ограничению в образовательных организациях доступа обучающихся к видам информации, распространяемой посредством сети "Интернет", причиняющей вред здоровью и (или) развитию детей, а также не соответствующей задачам образования;
- систематически повышает свою профессиональную квалификацию по направлению «Организация защиты детей от видов информации, распространяемой посредством сети «Интернет», причиняющей вред здоровью и (или) развитию детей, а также не соответствующей задачам образования, в образовательных организациях»;
- обеспечивает информирование организаций, отвечающих за работу технических и программных средств, об ошибках в работе оборудования и программного обеспечения;
- соблюдает правила и нормы охраны труда, техники безопасности и противопожарной защиты, правила использования сети Интернет;
- принимает участие в работе Экспертного совета по информатизации системы образования и воспитания при Временной комиссии Совета Федерации по развитию информационного общества.

3. Права

Вправе осуществлять действия организационно-административного характера для обеспечения ограничения доступа обучающихся к видам информации, распространяемой посредством сети "Интернет", причиняющей вред здоровью и (или) развитию детей, а также не соответствующей задачам образования, в образовательной организации.

4. Ответственность

Несет ответственность за ограничение доступа обучающихся к видам информации, распространяемой посредством сети "Интернет", причиняющей вред здоровью и (или) развитию детей, а также не соответствующей задачам образования, в образовательной организации.

Формулировки для внесения изменений в должностные инструкции отдельных сотрудников образовательных учреждений

В должностные инструкции сотрудников ОУ рекомендуется внести дополнительно следующие положения.

Педагогический работник (преподаватель/учитель/воспитатель)

1. Общие положения

Должен знать:

— дидактические возможности использования ресурсов сети Интернет;

— правила использования сети Интернет в ОУ.

— методические рекомендации по ограничению в образовательных организациях доступа обучающихся к видам информации, распространяемой посредством сети "Интернет", причиняющей вред здоровью и (или) развитию детей, а также не соответствующей задачам образования.

2. Должностные обязанности:

— планирует использование ресурсов сети Интернет в учебном процессе с учетом специфики преподаваемого предмета;

— разрабатывает, согласует с методическим объединением, представляет на педагогическом совете ОУ и размещает в информационном пространстве ОУ календарно-тематическое планирование;

— получает и использует в своей деятельности электронный адрес и пароли для работы в сети Интернет и информационной среде ОУ;

— использует разнообразные приемы, методы и средства обучения, в том числе по индивидуальным учебным планам в рамках федеральных государственных образовательных стандартов, современные образовательные технологии и сайты в сети «Интернет», включенные в Реестр безопасных образовательных сайтов;

— систематически повышает свою профессиональную квалификацию по направлению «Безопасное использование сайтов в сети «Интернет» в образовательном процессе в целях обучения и воспитания обучающихся в образовательной организации»;

— осуществляет контрольно-оценочную деятельность в образовательном процессе с использованием современных способов оценивания в условиях информационно-коммуникационных технологий (ведение электронных форм документации, в том числе электронного журнала и дневников обучающихся);

— соблюдает требования локальных нормативных актов образовательной организации;

— принимает участие в работе Экспертного совета по информатизации системы образования и воспитания при Временной комиссии Совета Федерации по развитию информационного общества.

3. Права

Вправе использовать в своей работе сайты сети «Интернет», включенные в Реестр безопасных образовательных сайтов.

4. Ответственность

Несет ответственность за ограничение доступа обучающихся к видам информации, распространяемой посредством сети "Интернет", причиняющей вред здоровью и (или) развитию детей, а также не соответствующей задачам образования, в ходе учебного процесса.

Примерный акт установки системы контентной фильтрации в образовательном учреждении

Всего компьютеров в ОУ			
Всего компьютеров, используемых в учебно-воспитательном процессе и подключенных к сети Интернет			
Инвентарный номер ПК	Наименование системы контентной фильтрации	Дата установки	ФИО, должность, подпись

(ФИО руководителя ОУ, подпись)

Рассмотрено
на заседании педагогического совета
протокол от _____

Утверждено
приказом директора _____
от _____

Акт проверки контентной фильтрации в

« ____ » _____ 20__ г.

№ _____

1. Общие сведения

Показатель	Значение
Количество компьютерных классов	
Общее количество компьютеров	
Количество компьютеров в локальной сети	
Количество компьютеров, подключенных к сети Интернет	
Провайдер	
Скорость передачи данных	

2. Информация о контент-фильтре

Действия, необходимые для обеспечения контентной фильтрации Интернет-ресурсов	Выполнение (да/нет)
Установлен контент-фильтр	
Название контент-фильтра	
Контент-фильтр работает на всех компьютерах, где есть доступ в сеть Интернет	

2. Результаты проверки работы системы контентной фильтрации

Категории запрещённой информации в образовательной организации	Возможность доступа (да/нет)
Перечень видов информации, запрещенной к распространению посредством сети «Интернет», причиняющей вред здоровью и (или) развитию детей, а также не соответствующей задачам образования согласно Методическим рекомендации по ограничению в образовательных организациях доступа обучающихся к видам	

информации, распространяемой посредством сети "Интернет", причиняющей вред здоровью и (или) развитию детей, а также не соответствующей задачам образования	
Интернет-ресурсы, не включённые в Реестр безопасных образовательных сайтов	

Члены комиссии по проведению проверки работы системы контентной фильтрации в образовательной организации:

Председатель комиссии _____ / _____
(подпись) (Ф. И. О.)

Члены комиссии _____ / _____
(подпись) (Ф.И.О.)

_____ / _____
(подпись) (Ф.И.О.)

С актом ознакомлен.

Директор _____ / _____
(подпись) (Ф.И.О.)

" ____ " _____ 20__ г.

Журнал контроля контентной фильтрации

Дата проверки	ФИО, должность проверяющего	Номер компьютера	Результаты проверки	Принятые меры	Подпись проверяющего

УТВЕРЖДАЮ

(Должность руководителя)

_____/_____
(Подпись) (Ф.И.О.)

(Дата)

Журнал регистрации случаев обнаружения сайтов

1. Дата обнаружения _____
2. Ф.И.О. и должность ответственного _____
3. Номер компьютера _____
4. Описание сайта в сети «Интернет», содержащего информацию, причиняющей вред здоровью и (или) развитию детей, а также не соответствующей задачам образования
5. Принятые меры
6. Подпись ответственного _____

1. Дата обнаружения _____
2. Ф.И.О. и должность ответственного _____
3. Номер компьютера _____
4. Описание сайта в сети «Интернет», содержащего информацию, причиняющей вред здоровью и (или) развитию детей, а также не соответствующей задачам образования
5. Принятые меры
6. Подпись ответственного _____

График работы точки доступа к сети Интернет

№ п/п	Дни недели	Занятость учащихся		Занятость педагогами	Администрация, сотрудники
		Урочное время	Внеурочное время		
1	Понедельник	8.00 – 18.30	10.00 – 12.00 14.00 – 17.00	8.00 - 19.00	8.00 - 19.00
2	Вторник	8.00 – 18.30	10.00 – 12.00 14.00 – 17.00	8.00 - 19.00	8.00 - 19.00
3	Среда	8.00 – 18.30	10.00 – 12.00 14.00 – 17.00	8.00 - 19.00	8.00 - 19.00
4	Четверг	8.00 – 18.30	10.00 – 12.00 14.00 – 17.00	8.00 - 19.00	8.00 - 19.00
5	Пятница	8.00 – 18.30	10.00 – 12.00 14.00 – 17.00	8.00 - 19.00	8.00 - 19.00
6	Суббота	8.00 – 12.00	10.00 – 12.00 12.00 – 14.00	8.00 – 15.00	8.00 - 15.00

Журнал № _____ учета доступа в сеть Интернет

Начат _____

Окончен _____

Ф.И.О. пользователя	Дата и время работы в Интернете	Цель работы в Интернете	Резолюция ответственного лица	Ф.И.О. ответственного лица	Подпись ответственного лица	Примечание

ФОРМЫ И ПЕРЕЧЕНЬ ЛИСТОВ ОЗНОКОМЛЕНИЯ

Лист ознакомления с инструкцией для сотрудников ОУ о порядке действий при осуществлении контроля над использованием обучающимися сети Интернет

№	Фамилия, имя, отчество	Должность	Дата	Подпись

**Лист ознакомления и согласия учащихся ОУ с правилами использования сети Интернет
в <наименование учреждения>**

№	Фамилия, имя, отчество	Класс	Дата	Подпись

**Лист ознакомления и согласия сотрудников ОУ с правилами использования сети Интернет
в <наименование учреждения>**

№	Фамилия, имя, отчество	Должность	Дата	Подпись



Навигатор методических ресурсов

(перечень рекомендуемой методической литературы
для использования заинтересованными лицами и организациями)

Иркутск, 2022

Навигатор методических ресурсов



Формирование информационной культуры и безопасности – процесс длительный и сложный, но важный и необходимый. Интернет – это всемирная энциклопедия, объединяющая информационные ресурсы во всем мире. Задача педагогов – сформировать разностороннюю интеллектуальную личность, высокий нравственный уровень которой будет гарантией ее информационной безопасности, система образования имеет большие возможности в данном направлении. Профессиональный и организационный ресурс этой системы, сфера ее социального влияния позволяют в рамках образовательной среды осуществлять комплексное и системное воздействие на установки, интересы и ориентиры всех участников образовательного процесса.

Специалистами ГКУ «Центр профилактики, реабилитации и коррекции» был проанализирован, обобщен, и систематизирован методический (международный, федеральный и региональный) опыт по данному вопросу. В помощь педагогам образовательных организаций подготовлен навигатор методических ресурсов специалиста в области профилактики.

Представленные пособия, методические рекомендации носят практический характер. Содержание материалов раскрывают феномен информационной безопасности, описание всех аспектов информационной безопасности, включающих теоретический и практический анализ рисков по информационным, потребительским, техническим и коммуникативным аспектам информационной безопасности, механизмы организации обучения обучающихся и их родителей (законных представителей).

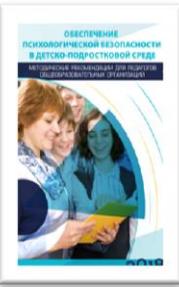
Использование «Навигатора методических ресурсов» позволит специалистам обеспечить комплекс профилактических мер, непрерывность и единство подходов в оказании помощи ребенку.

**С методическими материалами, представленными в навигаторе можно ознакомиться на сайте ГКУ «ЦПРК» цпрк.образование38.рф в разделе методическая копилка*

№	Название	Авторы	Аннотация	Режим доступа (электронная ссылка)
1.	 <p>Методические рекомендации «Интернет-безопасность детей»</p>	<p>Разработаны в рамках проекта «Безопасная интернет-среда — детям» фондом «Национальные ресурсы образования», 2019г.-44с.</p>	<p>Материалы отобраны для помощи в обучении подростков безопасному использованию Интернета и повышения их цифровой грамотности.</p>	<p>https://nro.center/wp-content/uploads/2019/10/rekomendacii.pdf</p>
2.	 <p>Методические рекомендации для руководителей общеобразовательных организаций «Обеспечение психологической безопасности образовательной организации»</p>	<p>Габер И.В., Зарецкий В.В., Артамонова Е.Г., Ефимова О.И., Калинина Н.В. — М.: ФГБНУ «Центр защиты прав и интересов детей», 2018. — 60 с.</p>	<p>Методические рекомендации подготовлены для руководителей общеобразовательных организаций. Разработаны в рамках реализации мероприятий плана первоочередных мер по повышению эффективности профилактики правонарушений обучающихся и обеспечению безопасности образовательных организаций.</p>	<p>http://xn--j1ajdw.xn--38-6kcadhwnl3cfdx.xn--p1ai/images/cms/data/mr_-_obespechenie_psihologicheskoy_bezopasnosti_obrazovatel_noj_sredy.pdf</p>
3.	 <p>Методические рекомендации для педагогов «Развитие устойчивости к интернет-рискам у детей и подростков»</p>	<p>Калинина Н.В. С 23 Развитие устойчивости к интернет-рискам у детей и подростков. Методические рекомендации для педагогов. М.: ФГБНУ «Центр защиты прав и интересов детей», 2018. — 11 с.</p>	<p>Методические рекомендации для педагогов общеобразовательных организаций, разработаны в рамках реализации мероприятий плана первоочередных мер по повышению эффективности профилактики правонарушений обучающихся и обеспечению безопасности образовательных организаций.</p>	<p>https://fcprc.ru/wp-content/uploads/2019/05/3-Razvitie-ustojchivosti-k-internet-riskam.pdf</p>

4.	 <p>Методичка для детей «Травли NET»</p>	<p>Петрановская Л. В., благотворительный Фонд «Галчонок» (грант Президента РФ на развитие гражданского общества, предоставляемого Фондом Президентских Грантов), 2019г.</p>	<p>Методическое пособие для детей по вопросам профилактики буллинга (кибербуллинга).</p>	<p>https://www.dropbox.com/s/go4cpg0pe4ddt71/A6%20Методичка%20для%20ДЕТЕЙ.pdf</p>
5.	 <p>Методические материалы по признакам девиаций, действиям специалистов системы образования в ситуациях социальных рисков и профилактике девиантного поведения обучающихся</p>	<p>Коллектив специалистов факультета Юридической психологии и Центра экстренной психологической помощи МГППУ, 2018г.</p>	<p>Для педагогов, классных руководителей и других специалистов образовательных организаций разработаны памятки по различным видам девиантного поведения и алгоритмы действий.</p>	<p>https://mgppu.ru/about/publications/deviant_behaviour</p>

6.		<p align="center">Брошюра «Безопасность детей в интернете»</p>	<p>Корпорация Microsoft</p>	<p>Брошюра для педагогов и родителей по вопросам безопасного поведения в сети интернет (профилактика кибербуллинга).</p>	<p>http://xn--j1ajdw.xn--38-6kcadhwnl3cfdx.xn--p1ai/images/cms/data/bezopasnost_detej_v_internete.pdf</p>
7.		<p align="center">Электронный справочник «Современные методы и технологии профилактики правонарушений несовершеннолетних»</p>	<p>Болелова А.Г. // Электронный журнал «Общество. Культура. Наука. Образование», 2016. Вып. 4.»</p>	<p>Электронный справочник рекомендован для специалистов системы профилактики безнадзорности и правонарушений несовершеннолетних, а также для использования в системе подготовки специалистов, волонтеров, работающих с детьми и подростками с криминальным и девиантным поведением.</p>	<p>http://xn--j1adv.xn--80aac0ct.xn--p1ai/media/2017/04/elektronnyj-spravochnik-fgbnu-tspvisppdm.pdf</p>
8.		<p align="center">Алгоритм действий для родителей обучающихся</p>	<p>АНО «Центр изучения и сетевого мониторинга молодежной среды» и ФГБУ «Центр защиты прав и интересов детей», 2020.</p>	<p>Методические рекомендации, включающие алгоритмы действий для родителей по раннему выявлению и реагированию на деструктивное поведение несовершеннолетних, проявляющееся под воздействием информации негативного характера, распространяемой в сети Интернет</p>	<p>https://mon.tatarstan.ru/rus/file/pub/pub_2510067.pdf</p>

9.		<p>Алгоритм действий для педагогов</p>	<p>АНО «Центр изучения и сетевого мониторинга молодежной среды» и ФГБУ «Центр защиты прав и интересов детей», 2020.</p>	<p>Методические рекомендации, включающие алгоритмы действий для педагогов по раннему выявлению и реагированию на деструктивное поведение несовершеннолетних, проявляющееся под воздействием информации негативного характера, распространяемой в сети Интернет</p>	<p>http://cppmsp52.ru/wp-content/uploads/2020/10/Методические-рекомендации-для-педагогов.pdf</p>
10.		<p>Методические рекомендации для психологов общеобразовательных организаций «Обеспечение психологической безопасности»</p>	<p>Авт.-сост.: Артамонова Е.Г., Ефимова О.И., Калинина Н.В., Салахова В.Б. — М.: ФГБНУ «Центр защиты прав и интересов детей», 2018 — 52 с.</p>	<p>Методические рекомендации предназначены для педагогов-психологов общеобразовательных организаций. Особое внимание в методических рекомендациях уделено рассмотрению вопросов профилактики девиантного поведения несовершеннолетних, предупреждению рисков и угроз их психологической безопасности, формированию ответственного поведения, сохранения жизни и здоровья.</p>	<p>http://xn--j1ajdw.xn--38-6kcadhwnl3cfdx.xn--p1ai/images/cms/data/mr_dlya_pedagogov-psihologov.pdf</p>
11.		<p>Методические рекомендации для педагогов общеобразовательных организаций «Обеспечение психологической безопасности в детско-подростковой среде»</p>	<p>Под ред. Л.П. Фальковской - М.: ФГБНУ «Центр защиты прав и интересов детей», 2018. — 32 с.</p>	<p>Методические рекомендации предназначены для педагогических работников общеобразовательных организаций: педагогов, классных руководителей, социальных педагогов. Большое внимание в методических рекомендациях уделено рассмотрению вопросов профилактики девиантного поведения несовершеннолетних, предупреждению рисков и угроз их психологической безопасности, формированию ответственного поведения, сохранения жизни и здоровья.</p>	<p>http://xn--j1ajdw.xn--38-6kcadhwnl3cfdx.xn--p1ai/images/cms/data/mr_obespechenie_psihologicheskoy_bezopasnosti_v_detskopodrostkovoj_srede.pdf</p>

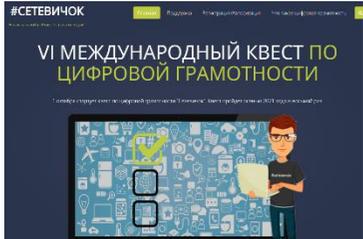
12.		<p>Журнал «Дети в информационном обществе»</p>	<p>Ежеквартальный научно-публицистический журнал, издается с 2009 года при научной поддержке Факультета психологии МГУ имени М. В. Ломоносова и Федерального института развития образования Министерства образования и науки РФ.</p>	<p>Журнал посвящен актуальным вопросам влияния современных инфокоммуникационных технологий на образ жизни, воспитание и личностное становление подрастающих поколений.</p>	<p>http://detionline.com/journal/numbers/32</p>
13.		<p>Азбука информационно й безопасности</p>	<p>Лаборатория Касперского</p>	<p>Брошюра для учеников младших классов «Азбука информационной безопасности».</p>	<p>http://www.ligainternet.ru/upload/docs/docs-for-dowload/Azbuka_informatsionnoy_bezopasnosti.pdf</p>
14.		<p>Интернет: возможности, компетенции, безопасность</p>	<p>Солдатова Г., Зотова Е., Лебешева М., Шляпников В. Интернет: возможности, компетенции, безопасность. Методическое пособие для работников системы общего образования. — М.: Google, 2013. — 165 с</p>	<p>Методическое пособие для работников системы общего образования. Методическое пособие «Интернет: возможности, компетенции, безопасность», состоящее из двух частей: лекций и практикума. Пособие направлено на повышение цифровой компетентности школьных учителей и практических психологов, расширение их представлений о возможностях Интернета, образе жизни и особенностях цифрового поколения, влиянии онлайн-рисков на развитие детей.</p>	<p>Теория - BookTheorie.pdf (detionline.com)</p> <p>Практика - http://detionline.com/assets/files/research/Book_Praktikum.pdf</p>

15.	 <p style="text-align: center;">Цифровая компетентность подростков и родителей</p>	<p>Цифровая компетентность подростков и родителей. Результаты всероссийского исследования / Г.У. Солдатова, Т.А. Нестик, Е.И. Расказова, Е.Ю. Зотова. — М.: Фонд Развития Интернет, 2013. — 144 с</p>	<p>В монографии рассматривается авторский подход к определению и диагностике цифровой компетентности личности в сетевом обществе. Представлены результаты первого общероссийского исследования цифровой компетентности подростков и родителей. Рассматриваются такие ее компоненты как знания, умения, мотивация и ответственность в разных сферах деятельности в интернете (работа с контентом, коммуникация, техносфера, потребление); показывается необходимость учета как отношения человека к интернету, так и особенностей его деятельности. Обсуждаются вопросы разработки образовательных программ по формированию и повышению цифровой компетентности у взрослых и подростков.</p>	<p style="text-align: center;">Всероссийское исследование цифровой компетентности 2013 — Дети России онлайн (detionline.com)</p>
16.	 <p style="text-align: center;">Родителям о психологической безопасности детей и подростков</p>	<p>Родителям о психологической безопасности детей и подростков. Памятка / Авт.-сост.: Артамонова Е.Г., Ефимова О.И., Калинина Н.В., Салахова В.Б. — 2-е изд. — М.: Группа МДВ, 2021. — 28 с</p>	<p>Памятка для родителей содержит просветительские и информационные материалы об особенностях и сложностях детско-подросткового возраста, рисках асоциального и суицидального поведения, интернет-угрозах и «ловушках». В памятке также представлены полезные ресурсы, на которых родители могут получить дополнительную информацию и консультацию специалистов по вопросам воспитания, развития и социализации детей.</p>	<p style="text-align: center;">https://fcprc.ru/wp-content/uploads/2019/05/4.Rodityam-o-psihologicheskoy-bezopasnosti-detej-i-podrostkov-pamyatka.pdf</p>



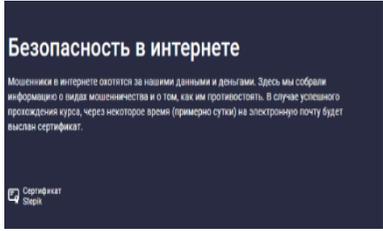
Список рекомендуемых интернет-ресурсов для организации и проведения работы по профилактике вовлечения несовершеннолетних посредством сети «Интернет» в противоправную деятельность

№	Сайт/ раздел/ аннотация	Целевая аудитория	Режим доступа
1.	 <p align="center">Единый урок</p> <p>Раздел: курсы повышения квалификации. Тема: Основы обеспечения информационной безопасности детей.</p>	Педагоги	https://www.единыйурок.рф/index.php/novosti
2.	 <p align="center">Изучи Интернет – управляй им!</p> <p>Социально-образовательный проект «Изучи Интернет – управляй им!» включает в себя образовательный модуль, где в игровой форме представлена информация об устройстве, возможностях и принципах функционирования Интернет, положение и итоги проведения ежегодного всероссийского онлайн-чемпионата для обучающихся.</p>	Обучающиеся	https://xn----7sbikand4bbyfwe.xn--p1ai/about/
3.	 <p align="center">Персональные данные. Дети</p> <p>Веб-сайт, посвященный правилам защиты персональных данных. Материалы (игры, тесты, мультимедиа) были разработаны специалистами Роскомнадзора.</p>	Обучающиеся	Персональные данные Дети (xn--80aalcbc2bocdadlpp9nfk.xn--d1acj3b)

4.	<p>Вебландия. Лучшие сайты для детей</p>  <p>«Веб-ландия» – это страна лучших ресурсов для детей. Каталог ресурсов включает разделы: «Игры и развлечения», «Животные и растения», «Искусство», «Спорт», «Иностранные языки», «Все о человеке» и другие. Каждый представленный веб-ресурс проходит строгий отбор, эксперты оценивают его безопасность, достоверность и другие параметры качества. Здесь можно принять участие в жизни «Вебландии»: вести обсуждения, делать записи в своем дневнике, предлагать лучшие, по вашему мнению, сайты.</p>	Обучающиеся	<p>ВебЛандия - лучшие сайты для детей (weblandia.ru)</p>
5.	<p>Разбираем Интернет</p>  <p>Проект «Разбираем Интернет» рассказывает об устройстве электронного мозга сетевого пространства и направлен на повышение цифровой компетентности учеников российских школ. Учебная часть проекта состоит из 4-х обучающих модулей для школьников. Для учителей - методическое пособие и практикум для проведения занятий. Интерактивная часть включает в себя игру и тестирование, которые призваны оценить уровень подготовки ученика. При успешном прохождении тестирования ученик награждается специальным сертификатом Google.</p>	Обучающиеся, педагоги, родители	<p>https://navigator.vbudushee.ru/direction/tsifrovaya-gramotnost/portal-razbiraem-internet/</p>
6.	<p>Сетевичок.рф</p>  <p>Предложен онлайн квест по цифровой грамотности.</p>	Обучающиеся	<p>http://сетевичок.рф/</p>

7.	 <p>Я-родитель</p> <p>Информационный интернет-портал при Фонде поддержки детей, находящихся в трудной жизненной ситуации. Основные задачи портала: профилактика жестокого обращения с детьми, помощь родителям в решении семейных проблем, знакомство с новыми методиками воспитания и работой социальных центров помощи семье и детям. На сайте Вы найдете новости социальной тематики, интересную и полезную информацию об особенностях воспитания детей в разном возрасте, о том, как своевременно заметить и развить таланты и способности ребенка, научитесь выбирать для малышей книги и игрушки. Узнаете, как разрешать сложные ситуации, сможете пройти психологические тесты, которые помогут вам лучше оценить себя как родителя. Специалисты в области детской и семейной психологии ответят на вопросы, касающиеся воспитания Вашего ребенка и ответственного родительства. Своим опытом Вы сможете поделиться на форуме и в блогах. Также на сайте проводятся онлайн консультации с психологами и юристами, в том числе и в видеоформате.</p>	Родители, педагоги	https://www.ya-roditel.ru/
8.	 <p>Федеральное государственное бюджетное учреждение «Центр защиты прав и интересов детей»</p> <p>является подведомственным учреждением Министерства просвещения Российской Федерации. Центр на протяжении 20 лет ведет свою деятельность, решая научно-методические, информационные, просветительские задачи в сфере сопровождения детей и подростков в образовательной среде. Также в фокусе внимания — педагогические работники, специалисты в области профилактики, родители (законные представители) несовершеннолетних обучающихся.</p>	Педагоги	https://fcprc.ru/

9.		<p align="center">Неделя «Кибербезопасности»</p> <p>В предложенном разделе собраны материалы, презентации для проведения занятий с обучающимися, родителями</p>	Родители, обучающиеся, педагоги.	http://itprojects.narfu.ru/cybersecurity/school-materials.php
10.		<p align="center">Мультпликационный фильм «Аркадий Паровозов спешит на помощь – Сомнительные сайты»</p>	Обучающиеся (1-4 классы)	https://www.rubiring.ru/arkady-parovozov-somnitelnyie-sayty/
11.		<p>В этом разделе находится подборка обучающих и развивающих видеоматериалов, которые помогут детям получить представление о приемлемых моделях поведения в Интернете. Все представленные здесь видеоролики в простой и доступной форме информируют юного пользователя сети о всевозможных аспектах взаимодействия с другими пользователями Интернета, о неоднозначных и затруднительных ситуациях, которые могут возникнуть во время пребывания в виртуальном пространстве, о том, как можно решить те или иные проблемы и куда можно обратиться в случае столкновения с недоброжелательностью и нарушением законов об информационной безопасности.</p>	Обучающиеся	http://i-deti.org/video/
12.		<p align="center">Центр безопасного интернета в России: подросткам.</p>	Родители, обучающиеся, педагоги.	http://www.saferunet.ru/teenager/

13.	 <p>Безопасность в интернете</p> <p>Мошенники в интернете охотятся за нашими деньгами и данными. Здесь мы собрали информацию о видах мошенничества и о том, как им противостоять. В случае успешного прохождения курса, через некоторое время (примерно сутки) на электронную почту будет выслан сертификат.</p> <p>Сертификат Stepik</p>	<p>Онлайн-курс «Безопасность в Интернете» от Академии Яндекса</p> <p>Онлайн курс, в котором собрана информацию о видах мошенничества в интернете и о том, как им противостоять, он будет полезен и родителям, а также учителям, планирующим рассказывать в школе о безопасном использовании интернета, например, во время Всероссийского урока по безопасности в интернете, или проводить уроки финансовой грамотности. В курсе три раздела. Каждый раздел состоит из конспекта для самостоятельного изучения, видео-урока и теста, помогающего лучше усвоить изученный материал.</p>	Обучающиеся (6-9 классы)	https://stepik.org/course/191/
14.	 <p>15 ПРАВИЛ БЕЗОПАСНОГО ПОВЕДЕНИЯ В ИНТЕРНЕТЕ</p> <p>Материал разработан специалистами Mail.Ru Group</p>	<p>15 правил безопасного поведения в интернете</p> <p>Правила составлены экспертами по кибербезопасности корпорации Mail.Ru Group и портала «Учеба.ру».</p>	Родители, обучающиеся, педагоги.	https://www.ucheba.ru/project/websafety
15.	 <p>Дети России Онлайн</p> <p>Скачайте материалы безопасности онлайн</p>	<p>Дети России онлайн</p> <p>На сайте представлены проекты: линия помощи «Дети онлайн», журнал «Дети в информационном обществе» и исследования Фонда Развития Интернет. Линия помощи «Дети онлайн» – это служба телефонного и онлайн консультирования для детей и взрослых по проблемам безопасного использования Интернет и мобильной связи. На линии помощи профессиональную психологическую и информационную поддержку оказывают психологи факультета психологии МГУ имени М. В. Ломоносова и Фонда Развития. Журнал «Дети в информационном обществе» – ежеквартальный научно-публицистический журнал, посвящен актуальным вопросам влияния современных инфокоммуникационных технологий на образ жизни, воспитание и личностное становление подрастающего поколения. Исследования Фонда Развития Интернет посвящены изучению психологии цифрового поколения России. Особое внимание уделяется проблемам безопасности детей и подростков в Интернет. С</p>	Педагоги, родители, обучающиеся	http://detionline.com/

<p>какими Интернет-угрозами сталкиваются дети и подростки России в сети и как их воспринимают? Насколько опасно отечественное киберпространство? Каковы способы защиты детей и подростков от рисков и опасностей глобальной «паутины»? Исследования затрагивают важнейшие вопросы современного этапа развития информационного общества в России, на которые необходимо обратить внимание специалистам по организации и проведению мероприятий по безопасному использованию Интернет</p>		
---	--	--

Приложение 5.

Памятки, полезные советы, правила для обучающихся, родителей и педагогических работников «Безопасный интернет»

ПАМЯТКА РОДИТЕЛЯМ ПО УПРАВЛЕНИЮ БЕЗОПАСНОСТЬЮ ДЕТЕЙ В ИНТЕРНЕТЕ

Интернет может быть прекрасным местом как для обучения, так и для отдыха и общения с друзьями. Но, как и весь реальный мир, Сеть тоже может быть опасна. Перед тем как разрешить детям выходить в Интернет самостоятельно, им следует уяснить некоторые моменты.

Расскажите своим детям об опасностях, существующих в Интернете, и научите правильно выходить из неприятных ситуаций. В заключение беседы установите определенные ограничения на использование Интернета и обсудите их с детьми. Сообща вы сможете создать для ребят уют и безопасность в Интернете. Если вы не уверены, с чего начать, вот несколько мыслей о том, как сделать посещение Интернета для детей полностью безопасным.

1. **Установите** правила работы в Интернете для детей и будьте непреклонны.
2. **Научите** детей предпринимать следующие меры предосторожности по сохранению конфиденциальности личной информации:
 - ✓ Представляясь, следует использовать только имя или псевдоним.
 - ✓ Никогда нельзя сообщать номер телефона или адрес проживания или учебы.
 - ✓ Никогда не посылать свои фотографии.
 - ✓ Никогда не разрешайте детям встречаться со знакомыми по Интернету без контроля со стороны взрослых.
 - ✓ **Объясните** детям, что разница между правильным и неправильным одинакова как в Интернете, так и в реальной жизни.
3. **Научите** детей доверять интуиции. Если их в Интернете что-либо беспокоит, им следует сообщить об этом Вам.
4. Если дети общаются в чатах, используют программы мгновенного обмена сообщениями, играют или занимаются чем-то иным, требующим регистрационного имени, **помогите** ребенку его выбрать и убедитесь, что оно не содержит никакой личной информации
5. **Научите** детей уважать других в Интернете.
6. **Убедитесь**, что они знают о том, что правила хорошего поведения действуют везде – даже в виртуальном мире.
7. **Настаивайте**, чтобы дети уважали собственность других в Интернете. Объясните, что незаконное копирование чужой работы – музыки, компьютерных игр и других программ – является кражей.
8. **Скажите** детям, что им никогда не следует встречаться с друзьями из Интернета. **Объясните**, что эти люди могут оказаться совсем не теми, за кого себя выдают.
9. **Скажите** детям, что не все, что они читают или видят в Интернете, – правда.
10. **Приучите** их спрашивать вас, если они не уверены.
11. **Контролируйте** деятельность детей в Интернете с помощью современных программ. Они помогут отфильтровать вредное содержимое, выяснить, какие сайты посещает ребенок и что он делает на них.
12. **Поощряйте** детей делиться с вами их опытом в Интернете. Посещайте Сеть вместе с детьми.
13. **Регулярно посещайте Интернет-дневник** своего ребенка, если он его ведет, для проверки.

Будьте внимательны к вашим детям!

ПАМЯТКА ДЛЯ ДЕТЕЙ ПО БЕЗОПАСНОМУ ПОВЕДЕНИЮ В ИНТЕРНЕТЕ

Для того чтобы обезопасить себя, свою семью, своих родителей от опасностей Интернета и причинения возможного ущерба, ребенок должен предпринимать следующие меры предосторожности при работе в Интернете:

1. Никогда не сообщайте свои имя, номер телефона, адрес проживания или учебы, пароли или номера кредитных карт, любимые места отдыха или проведения досуга
2. Используйте нейтральное экранное имя, не выдающее никаких личных сведений, в том числе и опосредованных: о школе, в которой вы учитесь, места, которые часто посещаете или планируете посетить, и пр.
3. Если вас что-то пугает в работе компьютера, немедленно выключите его. Расскажите об этом родителям или другим взрослым.
4. Всегда сообщайте взрослым обо всех случаях в Интернете, которые вызвали у вас смущение или тревогу.
5. Используйте фильтры электронной почты для блокирования спама и нежелательных сообщений.
6. Никогда не соглашайтесь на личную встречу с людьми, с которыми вы познакомились в Интернете. О подобных предложениях немедленно расскажите родителям.
7. Прекращайте любые контакты по электронной почте, в системе обмена мгновенными сообщениями или в чатах, если кто-нибудь начинает задавать вам вопросы личного характера.

Расскажите об этом родителям!!!

ВНУТРИСЕМЕЙНЫЕ ПРАВИЛА ИСПОЛЬЗОВАНИЯ ИНТЕРНЕТА

Перед тем как дети начнут осваивать Интернет, неплохо убедиться, что все понимают, что следует и чего не следует делать в Сети. Можно написать кодекс поведения, которому все согласны будут следовать. Кроме того, можно составить правила пользования для каждого ребенка в семье – в зависимости от их возраста. Каждый подписывает свое соглашение, чтобы показать, что понимает правила и соглашается следовать им в Интернете. Ниже приведен образец. Его можно скопировать, пересмотреть для нужд именно вашей семьи и напечатать для личного использования. Семейные правила пользования Сетью можно прикрепить около компьютера. Для напоминания.

СОГЛАШЕНИЕ О КОДЕКСЕ ПОВЕДЕНИЯ В ИНТЕРНЕТЕ.

Я обязуюсь: Обращаться к моим родителям, чтобы узнать правила пользования Интернетом: куда мне можно заходить, что можно делать и как долго позволено находиться в Интернете (___ минут или ___ часов).

Никогда не выдавать без разрешения родителей личную информацию: домашний адрес, номер телефона, рабочий адрес или номер телефона родителей, номера кредитных карточек или название и расположение моей школы.

Всегда немедленно сообщать родителям, если я увижу или получу в Интернете что-либо тревожащее меня или угрожающее мне; сюда входят сообщения электронной почты, сайты или даже содержимое обычной почты от друзей в Интернете.

Никогда не соглашаться лично встретиться с человеком, с которым я познакомился в Интернете, без разрешения родителей.

Никогда не отправлять без разрешения родителей свои фотографии или фотографии членов семьи другим людям через Интернет или обычной почтой.

Никогда никому, кроме своих родителей, не выдавать пароли Интернета (даже лучшим друзьям).

Вести себя в Интернете правильно и не делать ничего, что может обидеть или разозлить других людей или противоречить закону.

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

Никогда не делать без разрешения родителей в Интернете ничего, требующего оплаты.

Сообщить моим родителям мое регистрационное имя в Интернете и имена в чате, перечисленные ниже:

Имя (ребенок) _____

Родитель или опекун _____

Дата _____

Дата _____

Приложение 6.

Памятки, полезные советы, правила для обучающихся, родителей и педагогических работников по профилактике неблагоприятных для здоровья и обучения детей эффектов от воздействия устройств мобильной связи

Правила безопасного использования сотового телефона

1. Разговор по сотовому телефону не должен длиться более 2 минут, а минимальная пауза между звонками должна быть не менее 15 минут. Гораздо безопаснее писать SMS, чем держать трубку возле уха, так что по возможности лучше писать, чем говорить. Если телефон используется для игр, прослушивания музыки, чтения, необходимо перевести его в авиационный режим, когда нет связи с базовой станцией.

2. Держать трубку мобильного телефона нужно на расстоянии от уха, за нижнюю ее часть и вертикально. Затухание радиоволн пропорционально квадрату пройденного расстояния, поэтому, отодвинув трубку от уха всего на сантиметр и увеличив, таким образом, расстояние до мозга вдвое, можно понизить мощность, излучаемую в мозг, в четыре раза.

3. Подносить трубку к уху лучше после ответа на том конце. В момент вызова мобильный телефон работает на максимуме своей мощности независимо от условий связи в данном месте. В то же время через 10-20 секунд после начала вызова излучаемая мощность снижается до минимально допустимого уровня. Моментально прикладывать телефон к уху бессмысленно еще и потому, что первый длинный гудок появляется не сразу.

4. Многие дети часто отправляют SMS-сообщения или излишне увлекаются играми, встроенными в сотовые телефоны. Такое регулярное и длительное напряжение на растущие кисть и пальцы может вызывать различные нарушения костей и суставов. Кроме того, играя, ребёнок вынужден рассматривать мелкое изображение, долго смотрит на подсвеченный экран, всё время находящийся на одном расстоянии от глаз. Это является серьезной нагрузкой для глаз и может очень негативно повлиять на зрение.

5. Очки с металлической оправой при разговоре рекомендуется снимать: наличие такой оправы может привести к увеличению интенсивности электромагнитного поля, воздействующего на пользователя.

6. Существует несколько рекомендаций по хранению и переноске телефонов.

- ✓ Специалисты не советуют класть мобильные телефоны рядом с собой во время сна.
- ✓ Также не стоит постоянно держать мобильный телефон при себе, например, в кармане брюк. То есть, контакты с сотовым телефоном стоит ограничить, особенно, если в этом нет никакой необходимости. Носить мобильный телефон лучше в сумке, не стоит держать длительное время сотовый телефон на груди, поясе или в нагрудном кармане.

**ПАМЯТКА ДЛЯ ОБУЧАЮЩИХСЯ, РОДИТЕЛЕЙ И ПЕДАГОГИЧЕСКИХ
РАБОТНИКОВ ПО ПРОФИЛАКТИКЕ НЕБЛАГОПРИЯТНЫХ ДЛЯ
ЗДОРОВЬЯ И ОБУЧЕНИЯ ДЕТЕЙ ЭФФЕКТОВ ОТ ВОЗДЕЙСТВИЯ
УСТРОЙСТВ МОБИЛЬНОЙ СВЯЗИ**

1. Исключение ношения устройств мобильной связи на шее, поясе, в карманах одежды с целью снижения негативного влияния на здоровье.
2. Максимальное сокращение времени контакта с устройствами мобильной связи.
3. Максимальное удаление устройств мобильной связи от головы в момент соединения и разговора (с использованием громкой связи и гарнитуры).
4. Максимальное ограничение звонков с устройств мобильной связи в условиях неустойчивого приема сигнала сотовой связи (автобус, метро, поезд, автомобиль).
5. Размещение устройств мобильной связи на ночь на расстоянии более 2 метров от головы

*"Методические рекомендации об использовании устройств мобильной связи в общеобразовательных организациях" (утв. Роспотребнадзором N МР 2.4.0150-19, Рособрнадзором N 01-230/13-01 14.08.2019)

ПАМЯТКА ДЛЯ РОДИТЕЛЕЙ

Что делать, если ребенок зависим от телефона?

Как избавиться от зависимости телефона? Можно ли избежать возникновения зависимости от телефона? Однозначного ответа на эти вопросы, конечно, нет. А вот минимизировать вероятность ее появления и наметить пути искоренения – определенно можно. Рассмотрим наиболее действенные методы борьбы с зависимостью от телефона и Интернета у детей и подростков.

Личный пример родителей

Прежде всего важно понять, что гаджеты – неотъемлемая часть повседневной жизни современного подростка. Исходя из этого, воздействие по минимизации рисков возникновения зависимости от телефона или ее искоренение должно основываться на особых принципах, среди которых – личный пример.

Не стоит навязывать строптивому подростку какие-либо правила и открытые ограничения. Достаточно на опыте показать, что кроме смартфона и Интернета есть еще масса вещей, способных разнообразить повседневную жизнь.

Проводите время с ребенком. Если вы видите, что он чувствует себя одиноким или скучает, предложите ему вместе погулять в парке. Во время прогулки отключите свои мобильные устройства и уделите внимание ребенку.

Досуг, детские секции

Чрезмерное увлечение гаджетами говорит о том, что ребенок находится в поиске интересного занятия, которое сможет принести пользу и подарить положительные эмоции.

Альтернативой и отличным методом борьбы с зависимостью от телефона может стать посещение различного рода секций или же организация досуга, с учетом особых предпочтений и пожеланий ребенка. Так, отвлечься от гаджетов может помочь обычный конструктор, настольные игры или наборы для творчества, способные подарить массу незабываемых впечатлений.

Сделать мобильный телефон полезным

Не хочется, чтобы ребенок тратил время в пустую? Не знаете, что предпринять при зависимости от телефона? Попробуйте обратить ситуацию в лучшую сторону, сделайте так, чтобы гаджет стал полезнее.

При зависимости от телефона у детей, большее количество свободного времени тратится на сиделки в социальных сетях, изучение новостной ленты и, конечно, использование различного рода программ и приложений. Отличной возможностью сделать времяпровождение ребенка полезнее является установка обучающих программ. Отдельное внимание при этом стоит уделить играм для развития умственных способностей.

Ограничьте время использования телефона

Любое пагубное увлечение требует ограничения. Так должно происходить и с зависимостью от телефона. Чтобы ее побороть, необходимо установить временные лимиты использования гаджетов. Поощряйте ребенка, если он честно придерживается установленного расписания.

Важно, что в подростковый период сделать это достаточно трудно, однако вполне реально. Отличным помощником в этом может стать приложение родительского контроля.

Как известно, лучшим лечением любой болезни, в частности и зависимости от телефона, является ее профилактика. Чтобы снизить вероятность возникновения привычки постоянного использования гаджетов у детей, стоит своевременно установить дозволенные границы.

Приложения родительского контроля позволяет минимизировать вред от смартфона, обеспечивая возможность: удаленного контроля совершаемых действий (звонки/смс, использование приложений/социальных сетей и пр.); установки ряда ограничений на покупку, установку и использование приложений; блокировки вредоносных сайтов, на которых может содержаться неприемлемый контент; контроля времени использования гаджета как во время обучения, так и в свободный от занятий период.

Вы не одни

Если в итоге все приложенные усилия не принесут должного результата, обратитесь к психологу, который сможет предложить более профессиональный подход к решению проблемы. Обычно работа психолога с мобильной зависимостью ребенка состоит из трех составляющих: обучения здоровому использованию мобильных устройств, развития жизненно важных навыков и здорового образа жизни.

Наконец, если вы хотите отучить ребенка от пристрастия к мобильным устройствам, присмотритесь к собственному поведению. Возможно, вы увидите причину, по которой ребенок убегает в виртуальный мир. Покажите ребенку мир, который существует за пределами монитора его планшета. Позвольте ему испытать радость и удовольствие от простых вещей.

*Помните, дети – самое ценное, что есть в нашей жизни.
Безопасность ребенка – неотъемлемый компонент счастливой жизни родителей.*

Упражнения для профилактики развития синдрома запястного канала:

1. Сожмите руки в кулак, поддержите в течение 3 секунд, а затем максимально разожмите и подержите 6 секунд.
2. Вытяните руки перед собой, поднимите и опустите их.
3. Опишите кончиками пальцем круги, будто бы рисуя букву «О».
4. Сделайте круговые движения большими пальцами сначала влево, потом вправо.
5. Методично надавливайте одной рукой на пальцы другой.
6. Энергично несколько раз встряхните руки.

Комплексы упражнений для глаз (профилактика зрительного утомления)

Упражнения выполняются сидя или стоя, отвернувшись от экрана, при ритмичном дыхании, с максимальной амплитудой движения глаз.

Вариант 1:

1. Закрыть глаза, сильно напрягая глазные мышцы, на счет 1-4, затем раскрыть глаза, расслабив мышцы глаз, посмотреть вдаль на счет 1-6. Повторить 4-5 раз.
2. Посмотреть на переносицу и задержать взор на счет 1-4. До усталости глаза не доводить. Затем открыть глаза, посмотреть вдаль на счет 1-6. Повторить 4-5 раз.
3. Не поворачивая головы, посмотреть направо и зафиксировать взгляд на счет 1-4, затем посмотреть вдаль прямо на счет 1-6. Аналогичным образом проводят упражнения, но с фиксацией взгляда влево, вверх и вниз. Повторить 3-4 раза.
4. Перенести взгляд быстро по диагонали: направо вверх - налево вниз, потом прямо вдаль на счет 1-6; затем налево вверх направо вниз и посмотреть вдаль на счет 1-6. Повторить 4-5 раз.

Вариант 2:

1. Закрыть глаза, не напрягая глазные мышцы, на счет 1 - 4 широко раскрыть глаза и посмотреть вдаль на счет 1-6. Повторить 4-5 раз.
2. Посмотреть на кончик носа на счет 1 - 4, а потом перевести взгляд вдаль на счет 1-6. Повторить 4-5 раз.
3. Не поворачивая головы (голова прямо), делать медленно круговые движения глазами вверх- вправо-вниз-влево и в обратную сторону: вверх-влево-вниз-вправо. Затем посмотреть вдаль на счет 1-6. Повторить 4-5 раз.