

3. РЕКОМЕНДАЦИИ ДЛЯ РОДИТЕЛЕЙ (ЗАКОННЫХ ПРЕДСТАВИТЕЛЕЙ) ПО КИБЕРБЕЗОПАСНОСТИ ДЕТЕЙ И ПОДРОСТКОВ

Уважаемые родители!

В современном мире, насыщенном цифровыми технологиями, вопрос кибербезопасности становится все более актуальным. Дети и подростки активно используют Интернет для общения, учебы и развлечений, и важно, чтобы они понимали риски и умели защищать себя в виртуальном пространстве.

Проблема кибербезопасности заключается в том, что Интернет может быть источником не только полезной информации, но и угроз. Дети и подростки могут столкнуться в онлайн с мошенничеством, кибербуллинг, вредоносным контентом и другими опасностями. Это может привести к негативным последствиям для их психического здоровья, репутации и даже физической безопасности.

Нам, взрослым, необходимо уделять внимание вопросам кибербезопасности наших детей. Обсуждая с ними правила безопасного поведения и использования онлайн-пространства, объясняя, как распознавать те или иные риски, мы можем научить детей быть устойчивыми и защищенными в сети Интернет.

ВАЖНО

Медицинские и психолого-педагогические исследования, а также рекомендации СанПиН показывают, что использование электронных устройств и Интернета лучше **полностью исключить в раннем детстве (до 3 лет)**. Намного полезнее для детей живое общение, продуктивная развивающая деятельность, чтение, рисование и игры со сверстниками.

В старшем дошкольном возрасте экранное время может составлять **не более 1 часа в день** и только в присутствии взрослых. **В младшем школьном возрасте** продолжительность использования цифровых устройств **не должна превышать 1,5 часов**. **В подростковом и юношеском возрастах — не более 2 часов в день**.

При этом во всех возрастах непрерывный просмотр или онлайн-активность должны чередоваться с гимнастикой для глаз и другими видами интеллектуальной и физической деятельности. Каждый родитель, опираясь на рекомендации, стоит перед серьезным решением: определить, сколько времени пойдет его ребенку на пользу с учетом возраста, учебы, общения и отдыха.

Вы можете воспользоваться следующими простыми рекомендациями, чтобы помочь детям и подросткам быть более компетентными, осознанными, внимательными и осмотрительными в интернет-среде.



1 Обучайте детей и подростков основам кибербезопасности

- ✦ Поговорите с детьми о том, почему важно защищать личные данные и как это может помочь избежать проблем.
- ✦ Проверяйте настройки конфиденциальности и научите детей создавать надежные пароли, использовать двухфакторную аутентификацию и не делиться с незнакомцами личной информацией в Интернете.
 - **Надежный пароль** — это сложный пароль, состоящий из букв, цифр и символов. Обычно его трудно угадать или подобрать. Важно периодически менять пароли в мессенджерах, электронной почте и социальных сетях.
 - **Личная информация** — фамилия и имя, полная дата рождения, домашний адрес, номер телефона, номер школы и класса, информация о семье, другая личная информация (например, паспортные данные, данные медицинского полиса, СНИЛС и др.). Этими сведениями могут воспользоваться злоумышленники. Даже фото, видео и голосовые сообщения могут быть ими использованы.
- ✦ Используйте надежное антивирусное программное обеспечение на Ваших устройствах и регулярно обновляйте его. Обсуждайте с ребенком или подростком важность защиты от вредоносных программ.
- ✦ Рассказывайте о подозрительных людях в Интернете. Объясните ребенку или подростку, что не стоит общаться с незнакомцами в сети Интернет, и что делать, если кто-то ведет себя странно или пытается заставить делать что-то неприемлемое.
- ✦ Помогите детям и подросткам понять и осознать, почему не стоит отвечать на сообщения и звонки с незнакомых номеров по мобильной связи, в мессенджерах и социальных сетях. Объясните, что это может привести к нежелательным контактам и опасности.
- ✦ Обучайте распознаванию подозрительных ссылок. Расскажите ребенку или подростку о рисках перехода по ссылкам из неизвестных источников и научите его проверять ссылки перед переходом.

2 Обсуждайте и устанавливайте семейные правила использования Интернета и кибергигиены

- ✦ Определите вместе с ребенком или подростком, сколько времени он может проводить в Интернете, какие сайты он может посещать и с кем общаться, какие мессенджеры и социальные сети он может использовать.
- ✦ Если Ваш ребенок старшего дошкольного или младшего школьного возраста пользуется мобильным устройством или персональным компьютером, установите программы родительского контроля, чтобы ограничить доступ к нежелательному контенту и отслеживать активность в Интернете.
- ✦ Установите разумные ограничения на использование цифровых устройств и перерывы для других видов деятельности. Это поможет избежать переутомления и зависимости от Интернета.

3 Поддерживайте атмосферу доверия и регулярно обсуждайте с ребенком или подростком онлайн-опыт

- ✦ Поощряйте детей и подростков обсуждать с Вами вопросы, связанные с Интернетом и информационной безопасностью, делиться своими переживаниями, опасениями и проблемами, связанными с онлайн-пространством, без страха наказания. Проводите беседы о том, что делают дети в Интернете, с кем общаются, во что играют, какие сайты посещают, какой медиаконтент им интересен, и обсуждайте возможные риски. Рассмотрите возможность совместного просмотра контента и обсуждения увиденного.

4 Будьте примером для подражания

- ✦ Показывайте ребенку или подростку, как Вы сами соблюдаете правила информационной безопасности, и обсуждайте с ним Ваши совместные действия в Интернете. Показывайте, как правильно вести себя в Интернете, не нарушайте правила и нормы поведения в онлайн при ребенке, объясняйте, почему важно соблюдать эти правила.

5 Развивайте у детей навыки обращения за помощью и сообщения об опасности Вам и другим надежным взрослым (родственникам, учителям, сотрудникам правоохранительных органов)

- Обучайте детей и подростков тому, как фиксировать онлайн-риски с помощью скриншотов, сохранения видео- и аудиосообщений от незнакомцев. Все это может стать серьезной доказательной базой в критических ситуациях. Этот навык может помочь не только в виртуальном мире, но и в реальной жизни.

6 Помогайте детям и подросткам развивать критическое мышление

- Научите их анализировать информацию в Интернете, распознавать опасности: объясните, как распознавать мошенничество, кибертравлю и другие формы онлайн-угроз. Приводите примеры кибервиктимизации, ненадлежащего, рискованного и опасного онлайн-поведения, чтобы дети и подростки могли лучше понять, как избежать подобных ситуаций.
- Развивайте у ребенка аналитические навыки, чтобы он мог оценивать информацию в Интернете, сомневаться в достоверности источников и отличать достоверные источники от недостоверных. Расскажите, что не вся информация в Сети является правдивой.
 - Придумайте «волшебное слово-пароль», которое будете знать только Вы и Ваш ребенок, чтобы он мог распознать опасность: в случае, если ребенок ответил на сообщение или звонок незнакомца, с помощью этого слова ему будет проще распознать опасность.

7 Проявляйте поддержку и вовлеченность

- Постарайтесь быть вовлеченными в онлайн-активности: участвуйте в играх и социальных сетях вместе с детьми и подростками, чтобы лучше понять их интересы и окружение, это позволит поддерживать доверительный контакт с ними.
- Поощряйте детей и подростков заниматься безопасными и конструктивными офлайн и при необходимости онлайн-активностями, такими как образовательные игры, спорт или творческие проекты. Активная, интересная и насыщенная положительными эмоциями и событиями реальная жизнь — мощный источник позитивной самореализации без «бегства» в виртуальный мир.

8 Отработайте совместно с ребенком действия в ситуациях риска

- Важно заранее объяснить ребенку, как правильно действовать при столкновении с опасными онлайн-коммуникациями:
 - не вступать в перепалку, сразу заблокировать агрессора или мошенника, сохранить скриншоты переписки в качестве доказательств и обязательно рассказать о ситуации взрослым — родителям, учителю или обратиться в поддержку платформы, где произошел инцидент.
- Обращайтесь за помощью: если Вы заметили, что Ваш ребенок стал жертвой кибервиктимизации или проявляет опасное поведение в Интернете, не стесняйтесь обращаться за помощью к специалистам.

9 Регулярно обновляйте знания о кибербезопасности и кибергигиене, отслеживайте изменения в законодательстве и правилах платформ

- Следите за новостями и тенденциями в области кибербезопасности, изучайте новые методы защиты от киберпреступлений. Будьте в курсе изменений в законодательстве и правилах использования платформ, чтобы обеспечить максимальную защиту Вашего ребенка или подростка, адаптируйте свои подходы к обеспечению безопасности в соответствии с изменениями в Интернете.

Алгоритм действий родителя при обнаружении подозрительной онлайн-активности ребенка

- Обратите внимание на изменения в поведении ребенка или подростка. Если Вы заметили, что он стал более замкнутым, погруженным в онлайн, раздражительным или проявляет другие нетипичные для него эмоции, это может быть сигналом о проблемах в Интернете.
- Поговорите с ребенком. Выясните, что именно его беспокоит, и предложите свою помощь.
- Обратитесь за помощью к специалистам. Если Вы не можете самостоятельно решить проблему, обратитесь к психологу, социальному педагогу, психотерапевту или другим специалистам.

В ситуациях, когда ребенок сообщает Вам о совершенном в отношении него преступлении воспользуйтесь 8 памяткой [Навигатора профилактики виктимизации детей и подростков \(2024\)](#)



Более подробные рекомендации для родителей Вы найдете в пособии [«Риски в цифровой среде: диагностика, профилактика, коррекция»](#). — М: АНО «Центр глобальной ИТ-кооперации», 2024. — 152 с.



КУДА ОБРАТИТЬСЯ ЗА ПОМОЩЬЮ И ПОЛУЧИТЬ ДОПОЛНИТЕЛЬНУЮ ИНФОРМАЦИЮ



Телефоны доверия, горячие линии

- Горячая линия кризисной психологической помощи Министерства просвещения Российской Федерации 8-800-600-31-14**
 - На линии ежедневно и круглосуточно оказывается психологическая помощь и поддержка всем позвонившим, находящимся в кризисном состоянии или в кризисной ситуации (бесплатно, круглосуточно).
- Всероссийский Детский телефон доверия 8-800-2000-122**
 - Психологическое консультирование, экстренная и кризисная психологическая помощь детям, подросткам и родителям (бесплатно, круглосуточно).
- Горячая линия «Ребенок в опасности» Следственного комитета Российской Федерации 8-800-100-12-60#1**
 - Также для обращения доступна короткая комбинация 123 (бесплатно, круглосуточно).
- Горячая линия поддержки по вопросам травли Травли.NET 8-800-500-44-14**
 - ПН-ПТ с 10:00 до 20:00 по московскому времени.

Онлайн-помощь

- Горячая линия «Дети Онлайн» <http://detionline.com/helpline/about>
- ЧАТ-БОТ «Добрыня» (антибуллинг) <https://t.me/BylingBot>
- Сайт Молодежного цифрового омбудсмена, раздел «Цифропомощь» — сервис подачи обращений для молодых людей, которые столкнулись с проблемами в Интернете <https://youthombudsman.ru/help>
- Сообщить о запрещенном контенте можно на сайте Роскомнадзора <https://eais.rkn.gov.ru/feedback/>

Информационно-методические материалы и ресурсы

- Касперский детям <https://kids.kaspersky.ru/>

4. РЕКОМЕНДАЦИИ ДЛЯ СПЕЦИАЛИСТОВ ПО РАЗВИТИЮ МЕДИАКОМПЕТЕНЦИЙ У ДЕТЕЙ И ПОДРОСТКОВ

Уважаемые коллеги!

В современном мире цифровые технологии стали неотъемлемой частью нашей жизни. Но, как и любые инструменты, Интернет и различные устройства не только позволяют нам и нашим детям обретать новые знания, расширять возможности общения или проведения досуга, но и несут в себе различные онлайн-риски и угрозы. Поэтому важно, чтобы дети и подростки умели правильно и безопасно взаимодействовать с онлайн-средой.

Вы можете использовать данную памятку как основу для разработки профилактических, развивающих, психокоррекционных и просветительских программ, направленных на повышение осведомленности детей и подростков о рисках в Интернете, формирование навыков безопасного поведения в киберпространстве и развитие их медиакомпетенций.

Отметим, что профилактика в первую очередь направлена на развитие с учетом возрастных особенностей детей и подростков личностных ресурсов, способствующих преодолению различных трудных жизненных ситуаций и влияющих на повышение устойчивости к неблагоприятным факторам.

Поэтому с детьми и подростками целесообразно проводить занятия, которые в целом развивают такие ресурсы как:

- * когнитивные способности, интерес к учебе и духовному росту, чувство юмора,
- * просоциальные увлечения и широкий круг интересов,
- * эмоциональный интеллект и эмоциональная зрелость,
- * внутренний самоконтроль, целеустремленность, успешное овладение навыками принятия решений,
- * ответственное поведение и правосознание, уважение законов и норм общества, школы, семейных стандартов,
- * умение обращаться за помощью,
- * возможность активного участия в работе социальной группы,
- * доверительные отношения с родителями (законными представителями),
- * общение среди просоциальных сверстников и другие.



Помимо этого в процессе профилактики онлайн-рисков, опасного поведения детей и подростков в Интернете и в ходе развития медиакомпетенций у детей и подростков можно опираться на следующие рекомендации.

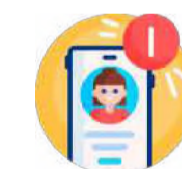
1 Обучение основам кибербезопасности и формирование навыков безопасного общения

- * Информируйте детей и подростков о принципах кибербезопасности: создании надежных паролей, использовании двухфакторной аутентификации, настройках конфиденциальности в социальных сетях и других онлайн-платформах.
- * Познакомьте детей с приложениями и инструментами, которые помогают оставаться в безопасности в Интернете, например, с программами родительского контроля, антивирусами и настройками конфиденциальности.
- * Проводите занятия, на которых можно обсудить правила безопасного общения в Интернете. Важно говорить об уважении к другим пользователям и недопустимости агрессивного поведения.



2 Развитие критического мышления и навыков анализа информации

- * Организуйте занятия, на которых дети и подростки смогут изучить основы критического мышления, включая анализ, оценку и интерпретацию данных.
- * Научите детей различать надежные и ненадежные источники информации, объясняя, какие факторы следует учитывать (авторитет, дата публикации, цель и т.д.).
- * Сформируйте навыки использования ресурсов и поисковых систем для поиска информации, проверки ее достоверности и фактов, приводите примеры фейковых новостей и дезинформации, чтобы помочь детям и подросткам понять, как они могут выглядеть и какие последствия они могут иметь.
- * Обсуждайте онлайн-контент: проводите занятия, на которых подростки смогут анализировать и обсуждать информацию из Интернета, включая новости, рекламу и социальные сети.
- * Развивайте навыки распознавания фейковых новостей: научите детей различать достоверные источники информации и фейковые новости, обсуждая примеры и методы проверки фактов.
- * Проводите дискуссии о социальных сетях: обсуждайте, как информация распространяется в социальных сетях, и как это может влиять на восприятие реальности.



3 Развитие навыков задавания вопросов

- * Научите детей задавать вопросы о том, что они читают или видят в Интернете. Например, «Кто это написал?», «Каковы его источники?» и «Почему это важно?».
- * Разработайте вместе с детьми список вопросов, которые они могут задавать при оценке информации.



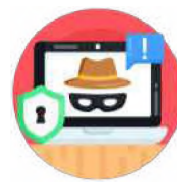
4 Осведомленность о рисках онлайн и офлайн

- ✦ Информировать о кибертравле и кибервиктимизации: обсуждайте с детьми и подростками, что такое кибербуллинг, как его распознать и как действовать в случае его возникновения.
- ✦ Обсуждайте реальные случаи: приводите с учетом возраста детей и подростков примеры кибервиктимизации и мошенничества, чтобы помочь им понять, как избежать подобных ситуаций.



5 Обучение распознаванию манипуляций в онлайн и офлайн

- ✦ Обсуждайте методы манипуляций, которые используют злоумышленники и мошенники: объясните, как используются эмоциональные триггеры, манипуляции и пропаганда для влияния на мнение людей.
- ✦ Анализируйте рекламные материалы: проводите занятия, на которых дети могут анализировать рекламу и пропаганду, чтобы понять, как они могут быть обмануты.



6 Развитие навыков саморегуляции

- ✦ Обучайте управлению временем: помогите детям и подросткам установить разумные лимиты на время, проведенное в Интернете, и научите их управлять своим временем.
- ✦ Поощряйте активный отдых: напоминайте детям и подросткам о важности физической активности и хобби вне Интернета, чтобы сбалансировать их активность в онлайн и офлайн.



7 Создание безопасной атмосферы для обсуждений и поддержка открытого общения

- ✦ Создайте атмосферу, в которой дети и подростки могут делиться своими переживаниями и проблемами, мыслями и сомнениями, связанными с Интернетом, без страха осуждения.
- ✦ Проводите регулярные беседы о том, что они делают в Интернете, с кем общаются, и какие у них есть вопросы или опасения, а также о том, что они читают и видят в онлайн-пространстве, и обсуждайте, как это может быть связано с реальностью.



8 Сотрудничество с родителями (законными представителями)

- ✦ Проводите семинары для родителей (законных представителей), чтобы они могли лучше понимать онлайн-риски и поддерживать своих детей в безопасном поведении в Интернете, в развитии у них критического мышления и распознавании недостоверной информации.



9 Использование интерактивных методов

- ✦ Включайте игры, дискуссии, групповые занятия и проекты, чтобы сделать обучение более увлекательным и запоминающимся.
- ✦ Используйте ролевые игры для отработки ситуаций, связанных с общением в Интернете, чтобы помочь детям научиться реагировать на потенциальные угрозы.



Подробные рекомендации по просвещению Вы найдете в пособии **«Организация просветительской работы с родителями по вопросам профилактики девиантного поведения»**. – Москва : ФГБОУ ВО МГППУ, 2018. – 112 с.



КУДА ОБРАТИТЬСЯ ЗА ПОМОЩЬ И ПОЛУЧИТЬ ДОПОЛНИТЕЛЬНУЮ ИНФОРМАЦИЮ

Телефоны доверия, горячие линии

- ✦ **Горячая линия кризисной психологической помощи Министерства просвещения Российской Федерации 8-800-600-31-14**
 - На линии ежедневно и круглосуточно оказывается психологическая помощь и поддержка всем позвонившим, находящимся в кризисном состоянии или в кризисной ситуации (бесплатно, круглосуточно).
- ✦ **Всероссийский Детский телефон доверия 8-800-2000-122**
 - Психологическое консультирование, экстренная и кризисная психологическая помощь детям, подросткам и родителям (бесплатно, круглосуточно).
- ✦ **Горячая линия «Ребенок в опасности» Следственного комитета Российской Федерации 8-800-100-12-60#1**
 - Также для обращения доступна короткая комбинация 123 (бесплатно, круглосуточно).
- ✦ **Горячая линия поддержки по вопросам травли Травли.NET 8-800-500-44-14**
 - ПН-ПТ с 10:00 до 20:00 по московскому времени.

Онлайн-помощь

1. Горячая линия «Дети Онлайн»
<http://detionline.com/help/line/about>
2. Раздел «Кибербуллинг» портала Минцифры и Ростелекома <https://xn----9sbbihqekoax4a5b.xn--p1ai/>
3. Сайт Молодежного цифрового омбудсмена, раздел «Цифропомощь»: сервис подачи обращений для молодых людей, которые столкнулись с проблемами в Интернете
<https://youthombudsman.ru/help>
4. Сообщить о запрещенном контенте можно на сайте Роскомнадзора <https://eais.rkn.gov.ru/feedback/>

Информационно-методические материалы и ресурсы

1. Образовательный портал Альянса по защите детей в цифровой среде «ЦИФРАтека. База практических знаний»
<https://cifrateka.ru/>
2. Вестник Киберполиции России
<https://max.ru/cyberpolice>
3. Касперский детям <https://kids.kaspersky.ru/>
4. Материалы АНО «Центр изучения и сетевого мониторинга молодежной среды»
<https://www.cism-ms.ru/poleznye-materialy/>

Куда можно направить родителей (законных представителей)

1. Портал Растимдетей.рф — навигатор для современных родителей по вопросам развития, воспитания и образования детей от 0 до 18 лет (статьи, памятки, буклеты).
2. Психологический университет для родителей «Быть родителем» — bytyeroditelem.rf