

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

Уважаемые родители!

В современном мире, насыщенном цифровыми технологиями, вопрос кибербезопасности становится всё более актуальным. Дети и подростки активно используют интернет для общения, учёбы 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, кибербуллингом, 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 в интернете и использования онлайн-пространства, объясняя, как распознавать те или иные риски, мы можем научить детей быть устойчивыми и защищенными в Сети.

ВАЖНО: медицинские и психолого-педагогические исследования, а также рекомендации СанПиН показывают, что использование электронных устройств и интернета лучше полностью исключить в раннем детстве. 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, а 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. При этом 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 ребёнком или подростком важность защиты от вредоносных программ.
- ★ Рассказывайте о подозрительных людях в интернете. Объясните ребёнку или подростку, что не стоит общаться с незнакомцами в сети и что делать, если кто-то ведёт 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 как по мобильной связи, так и в мессенджерах и социальных сетях. Объясните, что это может привести к нежелательным контактам и опасности.
- ★ Обучайте распознаванию подозрительных ссылок. Расскажите ребёнку 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 обсуждать с Вами вопросы, связанные с интернетом и информационной безопасностью, делиться своими переживаниями, опасениями и проблемами, связанными с интернетом, без страха наказания. Проводите беседы о том, что делают дети в интернете, с кем общаются, во что играют, какие сайты посещают и какой медиаконтент им интересен, и обсудите возможные риски. Рассмотрите возможность совместного просмотра контента и обсуждения увиденного.



4. Будьте примером для подражания.

- ★ Показывайте ребёнку 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 сети при ребёнке, 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 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. Помогите детям и подросткам развивать критическое мышление.

- Научите их анализировать информацию в интернете, распознавать опасности: объясните, как распознавать мошенничество, кибербуллинг и другие формы онлайн-угроз. Приводите примеры кибервиктимизации, ненадлежащего, рискованного и опасного онлайн-поведения, чтобы дети могли лучше понять, как избежать подобных ситуаций.
- Развивайте у ребенка аналитические навыки, чтобы он мог оценивать информацию в сети, 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, чтобы лучше понять их интересы и окружение, это позволит поддерживать доверительный контакт с ними.
- Поощряйте детей заниматься безопасными и конструктивными офлайн и при необходимости онлайн активностями, такими как образовательные игры 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 при обнаружении подозрительной активности

- 1 Обратите внимание на изменения в поведении ребенка или подростка. Если вы заметили, что он стал более замкнутым, раздражительным или проявляет другие нетипичные для него эмоции, это может быть сигналом о проблемах в интернете.
- 2 Поговорите с ребенком. Выясните, что именно его беспокоит, и предложите свою помощь.
- 3 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 родителю о совершенном в отношении него преступлении воспользуйтесь 8 памяткой **Навигатора профилактики виктимизации детей и подростков** (2024)



Более подробные рекомендации для родителей см. 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 (бесплатно, круглосуточно) 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.
 - Всероссийский Детский телефон доверия (бесплатно, круглосуточно) 8-800-2000-122.
Психологическое консультирование, экстренная и кризисная психологическая помощь детям, подросткам и родителям.
 - Горячая линия «Ребенок в опасности» Следственного комитета Российской Федерации (бесплатно, круглосуточно) 8-800-100-12-60#1. Также для обращения доступна короткая комбинация 123.
- 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/>