

8. КИБЕРРИСКОВАННОЕ ПОВЕДЕНИЕ

КИБЕРРИСКОВАННОЕ ПОВЕДЕНИЕ — это реализованное стремление несовершеннолетних к опасной неопределенности с использованием цифровых технологий. Такое поведение связано с возможностью наступления негативных последствий как для их безопасности, так и для их психоэмоционального состояния, несмотря на равную вероятность наступления положительного исхода.

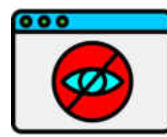
Среди киберрискованных действий можно выделить:

- 01 Общение с незнакомцами**
что может привести к риску киберагрессии, манипуляций, вовлечения в деструктивные сообщества или даже угроз (например, принятие запросов на дружбу от незнакомцев в социальных сетях или участие в чатах с незнакомыми людьми).
- 02 Публикация или отправка в сообщениях личной информации**
что может обуславливать кибервиктимизацию (примеры раскрытия личной информации: публикация фамилии и имени, полной даты рождения, домашнего адреса, номера телефона, номера школы и класса, информации о семье или других идентифицирующих данных).
- 03 Игнорирование настроек конфиденциальности**
в социальных сетях может привести к тому, что личная информация станет доступной для широкой аудитории (например, открытые профили в социальных сетях, где любой может видеть публикации и личные данные).
- 04 Кликавание на подозрительные ссылки**
которые ведут на вредоносные сайты или содержат вирусы (например, получение сообщений с подозрительными ссылками от незнакомцев или в результате фишинга).
- 05 Участие в опасных онлайн-играх или онлайн-квестах**
которые могут содержать элементы насилия или рискованные задания в офлайн, и могут быть опасны для здоровья и безопасности.
- 06 Использование ненадежных, недостоверных источников информации**
это может привести к распространению дезинформации или формированию неправильных представлений (например, дети и подростки могут верить в фейковые новости или участвовать в обсуждениях на форумах, где распространяется ложная информация).

Есть вероятность, что у несовершеннолетнего могут быть проблемы, если он:



использует специфический сленг. Следует иметь в виду, что сленг достаточно быстро меняется



стремится скрывать свою онлайн-активность или чрезмерно бравирует этим



принимает участие в группах и форумах, посвященных рискованной тематике (например, «Как быстро заработать» и т.д.)



на страницах в социальных сетях появляются соответствующие фотографии и видео (не обязательно свои)

ФОРМЫ КИБЕРРИСКОВАННОГО ПОВЕДЕНИЯ — онлайн форма (хотя в некоторых случаях подготовка может осуществляться офлайн) или смешанная форма (может начинаться в онлайн, переходить в офлайн, а результаты публиковаться в сети Интернет).

ПОДВИДЫ КИБЕРРИСКОВАННОГО ПОВЕДЕНИЯ СМЕШАННОЙ ФОРМЫ

1

Повторы онлайн-трендов

в том числе опасных и/или вирусных с последующей публикацией как подражание современным лидерам мнений (из жизни, видео и т.д.).



2

Просмотр шокирующих материалов (шок-контента)

в различных формах подачи (аудио, видео, текст), основная цель которых оказать сильное влияние на восприятие, вызвать душевные переживания и остаться в памяти как в день ознакомления с такой информацией, так и надолго, заставляя периодически воссоздавать запечатленный образ в сознании.

3

Опасное селфи и/или видео*

несовершеннолетний самостоятельно делает фотоснимок или видеозапись самого себя с помощью камеры мобильного или иного устройства в опасных для жизни условиях обычно с целью дальнейшей публикации в Интернете.

* Часто сочетается с рискованным поведением офлайн, которое может повлечь административную и уголовную ответственность, таким как:



- зацепинг** — способ передвижения, при котором человек цепляется за внешние элементы движущегося транспорта, может включать в себя *трейнсерфинг* (передвижение на крыше поезда), *трейнхоппинг* (запрыгивание на поезд), *фрейтхоп* (передвижение на грузовом поезде), *трейлсерфинг* (ездой между или под вагонами, на хвостовом вагоне или крыше поезда),
- крышолозание (руфинг)** — лазание по крышам высоких строений, небоскребов, многоэтажных жилых домов, а также по радиовышкам,
- диггерство** — незаконное исследование искусственных подземных коммуникаций или сооружений, например, бомбоубежищ, закрытых станций метро, бункеров и др.,
- сталкеринг** — посещение покинутых (заброшенных) объектов и мест, например, оставленных жилых домов, недостроенных зданий и иных мест,
- другие проявления рискованного экстремального досуга.

ПОДВИДЫ КИБЕРРИСКОВАННОГО ПОВЕДЕНИЯ ОНЛАЙН ФОРМЫ



1. Маргинальная видеотрансляция (трэш-стриминг)

ведущий за вознаграждение от зрителей выполняет их задания, при этом эфир потенциально пропагандирует насилие и жестокое обращение с людьми и/или животными, унижение человеческого достоинства.



3. Сексуализированная самопрезентация

форма самовыражения, при которой демонстрируется своя сексуальность через различные каналы, такие как социальные сети, мессенджеры или другие онлайн-платформы. Может включать в себя публикацию откровенных фотографий, видео, использование провокационных нарядов или языка, а также активное участие в обсуждениях на сексуальные темы. Данный подвид киберрискованного поведения увеличивает риски эксплуатации, груминга и виктимизации.



2. Рискованный онлайн-заработок

способы получения дохода в Интернете, которые могут быть связаны с высокими финансовыми, юридическими или репутационными рисками. Такие методы часто привлекают людей, обещая быстрые и большие прибыли, но могут привести к потерям или другим негативным последствиям.



4. Просмотр сексуализированных фото- и видеоматериалов (порнографии)

АЛГОРИТМ ДЕЙСТВИЙ СПЕЦИАЛИСТОВ

Что делать, если Вы точно знаете, что у обучающегося киберрискованное поведение:

- 01 Используйте общий алгоритм действий (памятка 0.4) данного Навигатора.
- 02 Проведите индивидуальную беседу с подростком с целью установления мотивации и оценки степени угрозы для его жизни и здоровья.
- 03 Установите связь с родителями (законными представителями) обучающегося. Если они не знают о его увлечениях, аккуратно объясните всю ситуацию, попросите их не ругать ребенка. Выработайте единую стратегию поведения. Возможно, семье нужна дополнительная психологическая и/или социальная помощь.
- 04 Вынесите этот случай на психолого-педагогический консилиум (ППК) с администрацией и другими специалистами образовательной организации (педагогом-психологом, социальным педагогом, другими специалистами). При необходимости иницилируйте Совет профилактики.
- 05 Выработайте индивидуальную траекторию помощи с обязательным привлечением родителей (законных представителей) обучающегося и возможным привлечением различных специалистов.

Основные принципы разговора с обучающимся:

- **до беседы** изучите тот вид деятельности, которым увлекается подросток,
- **во время беседы:**
 - ✳ используйте спокойный доброжелательный тон,
 - ✳ избегайте осуждения, оценивания и нравоучений. Дайте понять, что Вы, в первую очередь, беспокоитесь за его безопасность и не ставите своей целью наказать,
 - ✳ предоставьте подростку возможность высказаться, поделиться своими ощущениями и переживаниями по поводу его увлечений. Это поможет определить мотивацию и на основе этого выстроить план работы с этим подростком и/или его семьей,
 - ✳ убедитесь в том, что подросток полностью осознает, как административные риски, так и опасность для жизни и здоровья. Для этого задавайте открытые вопросы (например, «Как ты считаешь, есть ли какая-то опасность в твоих увлечениях?», «Может ли это причинить кому-то вред? Кому? Какой вред?» и т.д.)

В случае сочетания киберрискованного поведения с другими видами рискованного поведения также используйте 8 памятку [Навигатора профилактики девиантного поведения \(2022\)](#)



КУДА ОБРАТИТЬСЯ ЗА ПОМОЩЬЮ

- ✳ **Всероссийский Детский телефон доверия** (бесплатно, круглосуточно) **8-800-2000-122**
 - Психологическое консультирование, экстренная и кризисная психологическая помощь для детей в трудной жизненной ситуации, подростков и их родителей, педагогов и специалистов в организациях Вашего муниципального образования/субъекта Российской Федерации.
- ✳ **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.

- ✳ **Горячая линия «Дети Онлайн»**
<http://detionline.com/helpline/about>

- ✳ **ЧАТ-БОТ «Добрыня» (антибуллинг)**
<https://t.me/BylingBot>



КУДА МОЖНО НАПРАВИТЬ РОДИТЕЛЕЙ (ЗАКОННЫХ ПРЕДСТАВИТЕЛЕЙ)

1. Портал [Растимдетей.рф](http://rastimdetey.rf) — 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» — bytyroditeljem.rf

1. РЕКОМЕНДАЦИИ ДЛЯ ДЕТЕЙ ПО БЕЗОПАСНОСТИ В СЕТИ ИНТЕРНЕТ

Привет, дорогой друг!

Дети и взрослые используют разные устройства, чтобы общаться и узнавать много нового в Интернете. Но важно пользоваться им очень аккуратно.

Если ты с разрешения родителей во время учебы или отдыха используешь Интернет, следуй правилам, которые описаны ниже. Они помогут тебе быть внимательным и осторожным в онлайн-сети, а также заботиться о себе, своих близких, друзьях и других людях.

1 Используй Интернет только с разрешения родителей и будь осторожен онлайн. Старайся ограничить время, проведенное в Интернете. Делай перерывы, чтобы не переутомляться. И занимайся другими видами деятельности.



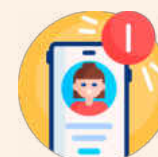
2 Обсуждай с родителями и близкими взрослыми те развлекательные сайты, мессенджеры или игры, в которых хочешь зарегистрироваться или которые используешь.



3 Вместе с родителями настрой в телефоне, на планшете или компьютере конфиденциальность: спрячь свою личную информацию, пусть ее видят только близкие, друзья и учителя.



4 Не публикуй в Интернете личную информацию: не пиши свою фамилию, имя, дату рождения, номер телефона, свой домашний адрес и номер школы. Исключение составляют только чаты с родителями или школьные чаты с учителями.



5 Не выкладывай в Интернете свои фото, видео или голосовые сообщения – ими могут воспользоваться злоумышленники.



6 Если у тебя есть страница или канал в социальных сетях, которые ты ведешь с разрешения родителей, ограничь доступ к своим публикациям для посторонних людей. Попроси родителей помочь тебе настроить их так, чтобы твои посты могли видеть только те, кому ты доверяешь (родители, близкие родственники, друзья, возможно, учителя).



7 Попроси родителей научить тебя создавать сложные пароли: пароль должен состоять из букв, цифр и специальных символов.



8 Не используй один и тот же пароль для разных приложений. Регулярно меняй пароли. Никогда не делись своими паролями с другими, даже с друзьями, пароль должны знать только родители.



9 Регулярно напоминай родителям обновлять антивирус на твоих устройствах, он защищает от вирусов и нежелательных программ. Но антивирусные программы должны выбирать взрослые.



10 Будь вежлив в Интернете с другими пользователями, если ты общаешься в чатах, например, чате класса.



11 Обсуждай с родителями или учителями ситуации, с которыми ты сталкиваешься в Интернете, и которые тебя тревожат или пугают. Обязательно прекрати общение и расскажи об этом родителям или учителям, если кто-то в Интернете:

- обижает тебя, или ты чувствуешь себя там не так, как хочешь (например, неудобно или неприятно),
- ведет себя странно, расспрашивает о твоей семье или просит сделать что-то плохое или постыдное.



- 12 Не общайся с незнакомыми людьми и не принимай их в друзья,** если у тебя есть мессенджеры или социальные сети. Не принимай от них и не отправляй им личные сообщения. Общайся только на проверенных родителями платформах.
- 13 Если в Интернете случилось что-то плохое,** например, кто-то написал тебе что-то обидное или ты увидел что-то нехорошее в Интернете, сохрани это как картинку или сообщение, чтобы показать близким взрослым.
- 14 Если с разрешения родителей ты играешь в онлайн-игры,** то используй псевдоним, то есть выдуманное, а не настоящее имя.
- 15 Обсуждай с родителями, в какие игры ты играешь и что смотришь в Интернете.** В играх и видео в Интернете иногда показывают плохое поведение или говорят плохие слова. Выбирай вместе с родителями только безопасные сайты, игры и видео. Всегда спрашивай взрослых, если что-то непонятно.
- 16 Не всему в Интернете можно доверять.** Проверяй вместе с родителями или учителями информацию и источники, особенно новости и заманчивые предложения. Избегай подозрительных ссылок и сообщений, чтобы не скачать вирусы или не попасть на обман.
- 17 Совершай покупки в Интернете только вместе с родителями.** Не покупай ничего в личных сообщениях в социальных сетях или мессенджерах — так мошенники могут украсть деньги или доступ к твоим аккаунтам.
- 18 Никогда не сообщай никому кроме родителей ПИН-код банковской карты и коды из СМС-уведомлений.**
- 19 Участвуй только в тех онлайн-занятиях, которые разрешают и предлагают родители и учителя.** Это могут быть олимпиады, конкурсы, курсы или вебинары.



Эти правила помогут тебе защитить себя от различных неприятностей в Интернете, а также создать безопасное и позитивное пространство для себя и других.

КУДА ОБРАТИТЬСЯ ЗА ПОМОЩЬЮ

Если что-то тебя настораживает или пугает – обязательно обратись к родителям или учителям за поддержкой и помощью!

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**
- ✳ **Горячая линия поддержки по вопросам травли Травли.NET** **8-800-500-44-14** (ПН-ПТ с 10:00 до 20:00 по московскому времени).

2. РЕКОМЕНДАЦИИ ДЛЯ ПОДРОСТКОВ ПО БЕЗОПАСНОСТИ В СЕТИ ИНТЕРНЕТ

Привет, дорогой друг!

Современный мир стремительно меняется, развиваются онлайн-технологии, различные гаджеты и девайсы, которые все мы используем в повседневной жизни. Интернет также стал некоторой частью нашей реальности и инструментом, с помощью которого можно общаться, учиться, узнавать новое. И, как с любым инструментом, им нужно пользоваться аккуратно, помня о некоторых рисках и угрозах виртуального мира.

Если ты во время учебы или досуга используешь Интернет и его ресурсы на смартфоне, планшете или персональном компьютере, пожалуйста, воспользуйся следующими рекомендациями. Они помогут тебе быть более компетентным, осознанным, внимательным и осмотрительным в онлайн-пространстве, проявить заботу о себе, своих близких и других людях.

1 Помни о защите своей личной информации

Не делись в онлайн своими или чужими личными данными: никогда не публикуй свои фамилию и имя, полную дату рождения, домашний адрес, номер телефона, номер школы и класса, в которых учишься, информацию о семье или другую личную информацию в Интернете. Этими сведениями могут воспользоваться злоумышленники. Даже твои фото, видео и голосовые сообщения могут быть ими использованы. Используй никнеймы (псевдонимы) при регистрации на сайтах, в социальных сетях, мессенджерах или в играх, а не свое настоящее имя.



ИСКЛЮЧЕНИЕ: официальные платформы (например, Федеральная государственная информационная система «Единый портал государственных и муниципальных услуг» или Госуслуги) и мессенджеры (например, Сферум, Max).

2 Используй настройки конфиденциальности

На мобильных устройствах, в мессенджерах, социальных сетях, чтобы ограничить доступ к твоей информации. Убедись, что твои профили и аккаунты настроены так, чтобы только близкие, друзья и учителя могли видеть личную информацию. Если ты активно ведешь свою страницу, канал или паблик, ограничь доступ к своим постам: настрой видимость своих публикаций так, чтобы их могли видеть только те, кому ты доверяешь (родители, близкие родственники, друзья, возможно учителя).



3 Применяй безопасные пароли и не сообщай их никому

Надежный пароль — это сложный пароль, состоящий из заглавных и строчных букв, цифр и символов. Обычно его трудно угадать или подобрать. Не используй один и тот же пароль для разных аккаунтов. Никогда не делись своими паролями с другими, даже с друзьями. Регулярно меняй пароли, чтобы обезопасить себя.



4 Используй антивирусное программное обеспечение и фаервол (межсетевой экран, брандмауэр)

Для защиты от вредоносных программ и нежелательного трафика используй антивирусы и системы безопасности, которые действуют как барьер между компьютерной сетью и внешним миром.



5 Обсуждай вопросы онлайн-безопасности с родителями или учителями

Сообщай о проблемах: если кто-то угрожает тебе или ты чувствуешь себя некомфортно в Интернете, расскажи об этом родителям или учителям. Обращаться за помощью и принимать ее — важный навык современного человека.

Сохраняй доказательства: если ты стал жертвой кибертравли (кибербуллинга), другого онлайн-насилия или мошенничества, сохраняй скриншоты и сообщения как доказательства. Помни о кибербуллинге: если ты стал жертвой онлайн-травли, сообщи об этом взрослым.

Будь внимателен к онлайн-играм или медиаконтенту: некоторые игры могут содержать агрессивное поведение, а видео и фото — неподобающий, токсичный контент. Обсуждай с родителями, в какие игры ты играешь, какие онлайн-платформы и контент тебе интересны.



6 Старайся придерживаться безопасного общения

Интернет так устроен, что иногда может сложиться иллюзия доверия, безопасности, анонимности и конфиденциальности. Может показаться, что ты хорошо знаешь человека, с которым в реальной жизни никогда не встречался, но уже какое-то время общаешься онлайн. Но это может быть небезопасным. Поэтому не общайся с незнакомыми людьми в Интернете и не принимай запросы в друзья от тех, кого не знаешь в реальной жизни. Не отправляй личные сообщения незнакомцам: будь осторожен с тем, что ты пишешь и отправляешь в личных сообщениях. Не встречайся с людьми из Интернета, это могут быть злоумышленники.

Если кто-то в Интернете ведет себя странно или пытается заставить тебя делать что-то, что вызывает у тебя стыд, или спрашивает тебя о том, о чем ты не хочешь говорить, задает много вопросов о твоей семье, прекрати общение и сообщи об этом взрослым. Самый надежный способ позаботиться о себе — прервать контакт с незнакомым пользователем, который может писать или звонить тебе.



7 Позаботься о своей кибергигиене

Старайся ограничить время, проведенное в Интернете. Делай перерывы и занимайся другими видами деятельности, чтобы избежать переутомления, усталости глаз и зависимости от цифровых устройств.

8 Участвуй только в безопасных онлайн-активностях

Выбирай безопасные сайты и приложения, используй только проверенные платформы для общения и игр. Участвуй в тех образовательных онлайн-активностях (олимпиадах, конкурсах, курсах, вебинарах и других событиях), которые проверены твоими близкими взрослыми, и которые помогут тебе развивать навыки и знания.



9 Развивай критическое мышление

Проверяй и перепроверяй информацию: не верь всему, что видишь в интернете. Проверяй факты и источники информации, особенно если это касается новостей или заманчивых предложений.

Будь осторожен с рекламой: не кликай на подозрительные ссылки, которые могут привести к вирусам или мошенничеству. Помни, что ссылки из подозрительных писем, сообщений и постов в мессенджерах или социальных сетях могут содержать вредоносное программное обеспечение и заразить твой компьютер или мобильное устройство.

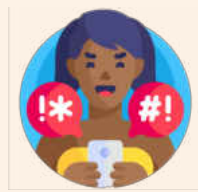


10 Будь бдителен при онлайн-покупках

Не доверяй сайтам, которые выглядят подозрительно, и проверяй отзывы о продавцах перед покупкой товаров онлайн. Совершай покупки только вместе с родителями.

Не делай покупки в личных сообщениях в мессенджерах или социальных сетях: мошенники могут получить доступ и контроль к денежным средствам и твоим аккаунтам.

Будь предельно осторожен с предложениями сделать донат (добровольное денежное пожертвование).



11 Никогда не продавай свои аккаунты в мессенджерах, социальных сетях, онлайн-играх, а также СИМ-карты и банковские карты!

Мошенники могут воспользоваться ими в корыстных целях, но ответственность придется нести тебе, твоим родителям и близким. Никогда не сообщай номер, ПИН-код, CVC-код и другие данные своей банковской карты, а также коды из СМС-уведомлений и электронных писем посторонним людям.



12 Изучи правила и нормы поведения в Интернете

Придерживайся правил, чтобы избежать конфликтов и неприятных ситуаций. Соблюдай законы, действующие в нашей стране — они также распространяются на поисковые запросы, поведение людей в Интернете и публикуемый ими контент.

Будь осторожен с публикациями в социальных сетях и сообщениями в мессенджерах. То, что кажется забавным или безобидным, может нарушать закон, или оказаться вирусным и быстро распространиться среди большой, не всегда желательной, аудитории. Прежде чем разместить пост или отправить сообщение, внимательно оценивай его содержание. **Помни:** Интернет — это публичное пространство, и необдуманные поступки могут иметь серьезные последствия.

Если ты столкнулся с противоправным контентом в Интернете, сообщи об этом родителям и/или учителям, а также отправь ссылки и скриншоты в правоохранительные органы и Роскомнадзор.



Кибербезопасность, цифровая грамотность, навыки распознавания онлайн-рисков — это важный аспект твоей жизни в современном мире!

Следуя этим рекомендациям, ты сможешь защитить себя от различных онлайн-угроз, а также создать безопасное и позитивное онлайн-пространство для себя и других.

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/>

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, 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 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.

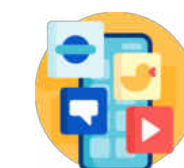
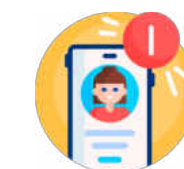
1 Обучение основам кибербезопасности и формирование навыков безопасного общения

- ✳ 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

- ✳ Информируйте 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/helpline/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