**Возрастные рекомендации при использовании сети Интернет**

В дополнение к общим, существуют также возрастные рекомендации, которые следует учитывать при использовании интернета детьми.

**2 – 4 года**

* Не допускайте самостоятельного времяпрепровождения в интернете.
* Не допускайте никаких пугающих изображений, ни реальных, ни вымышленных.
* Не позволяйте детям переходить по ссылкам.
* Ограничьте время, проводимое за компьютером.
* Прививайте базовые навыки работы с компьютером с помощью соответствующих возрасту игр и образовательных программ.

**5 – 7 лет**

* Не допускайте самостоятельного времяпрепровождения в интернете или с телефоном.
* Не допускайте никаких пугающих изображений, ни реальных, ни вымышленных.
* Не позволяйте детям переходить по ссылкам.
* Используйте удобные для детей поисковые системы с родительским контролем.
* Настройте фильтры по возрасту.
* Ограничьте время, проводимое в интернете.
* Ограничьте детей списком любимых сайтов, который вы составите вместе.
* Убедитесь, что подключенные к интернету устройства находятся в открытом доступе, где вы можете их наблюдать.
* Заблокируйте использование средств обмена мгновенными сообщениями, электронной почты, чатов, мобильного интернета, обмена текстовыми, графическими и видео сообщениями, а также доступ к доскам сообщений.
* Научите детей никогда не разглашать личную информацию в интернете.

Важно осознавать риски и разрешать детям использовать только приложения, соответствующие их возрасту и обстоятельствам.

В этой статье описаны потенциально опасные для детей приложения и веб-сайты.

Итак, как обезопасить детей в Интернете?

Давайте посмотрим, как какие меры можно принять, чтобы оградить их от повседневных опасностей, поджидающих их в Сети.

## Блокировка сайтов с ненадлежащим контентом

Не секрет, что далеко не все сайты предназначены для просмотра детьми. Ваш ребенок может случайно наткнуться на сайт с ненадлежащим контентом просто через запрос в поисковой системе или пройдя по ссылке, которую отправил приятель.

Как можно обеспечивать безопасность своих детей в Интернете и в то же время не оказывать на них чрезмерного давления?

Ответом может стать функция Родительского контроля. Она доступна и как отдельное решение, и в составе комплексных защитных решений.

Функция «безопасный поиск» в Родительском контроле блокирует неприемлемый контент, а большинство решений также предоставляют родителям подробные отчеты, о том, что делает их ребенок в Интернете.

Но иногда именно безопасные сайты могут испортить виртуальную игровую площадку.

## Не вступайте в разговоры с незнакомыми людьми

Ваш ребенок с удовольствием играет в новейшую онлайн-игру с друзьями, общаясь с ними через чаты?

Но в этих чатах также есть киберпреступники, которые прячутся за аватарами, стараясь обманом вынудить ваших детей раскрыть личную информацию.

Эта информация затем может использоваться для кражи ваших идентификационных данных и денег.

Игра в известные игры или игры на проверенных сайтах может помочь защитить вашего ребенка.

Но даже в этом случае вам будет сложно защитить своего ребенка в Интернете, просто отслеживая, с кем и о чем он разговаривает онлайн.

Помогут защитные продукты, такие как [Kaspersky Total Security](https://www.kaspersky.ru/total-security), которые не позволяют ребенку отправлять через чаты и мессенджеры личную информацию, например, номер банковского счета, имена и адреса.

И в этих чатах «обитают» не только киберпреступники. К сожалению, как и в реальной жизни, в Интернете ребенок может стать жертвой онлайн-издевательств.

## Не поддавайтесь онлайн-буллингу

На игровых сайтах некоторые участники играют, просто чтобы провоцировать и издеваться над другими игроками. Таких называют «[кибербулли](https://www.kaspersky.ru/about/press-releases/2015_ugroza-detjam-o-kotoroj-ne-znajut-vzroslye)».

Контролировать и предотвращать интернет-травлю в видеоиграх сложно. Как правило, модераторы пытаются блокировать хулиганов, но при большом количестве игроков невозможно уследить за каждым.

И здесь опять на помощь придут функции родительского контроля. Они отслеживают, с кем ваш ребенок общается онлайн, и позволяют вам блокировать любые нежелательные контакты.

Вы также можете получать предупреждения, когда какое-либо из обозначенных вами слов используется в онлайн-коммуникации.

Обратите внимание: даже при такой защите все равно невозможно полностью контролировать действия своего ребенка в Интернете.

Безобидные на первый взгляд сайты могут содержать вредоносные ссылки, поставят под угрозу безопасность всей вашей сети.

## Не скачивайте вирус

Киберпреступники знают, что дети часто ищут в Сети бесплатное ПО, музыку и игры. Они также знают, что дети часто доверяют [ссылкам и вложениям электронной почты](https://www.kaspersky.ru/resource-center/threats/spam-phishing).

Если ваш ребенок пройдет по одной из этих ссылок, он может загрузить вирус, который не поставит под угрозу безопасность не только его компьютера, но всей вашей сети.

Ребенок может сделать это непреднамеренно: он всего лишь кликнул на рекламный баннер, а [вредоносное ПО](https://www.kaspersky.ru/resource-center/threats/computer-viruses-and-malware-facts-and-faqs) уже незаметно загружается на его компьютер и угрожает его безопасности.

В любом случае, лучшая защита - это надежное защитное решение, которое блокирует небезопасные ссылки и проверяет каждую скачиваемую программу на наличие признаков вредоносного ПО.

Комплексный защитный продукт, такой как [Kaspersky Total Security](https://www.kaspersky.ru/total-security), сделает это для каждого члена вашей семьи.

Вы можете контролировать всю домашнюю сеть с вашего компьютера и настраивать параметры безопасности для каждого устройства по отдельности.

## Обеспечение безопасности детей в Интернете - это приоритет номер один

Ничто не заменит участие родителей, когда дело касается безопасности детей в Интернете.

Просто разговаривайте с вашими детьми, научите их не нажимать автоматически кнопку «да» и не поддаваться на провокации кибер-хулиганов или потенциальных киберпреступников.

Защитные решения дополняют эту работу, контролируя поведение ребенка в Интернете, что обеспечивает безопасность игровой онлайн-площадки.

Комплексные защитные решения также позволяют удаленно контролировать и управлять всеми компьютерами в вашей домашней сети с вашего устройства.

В конце дня детям нужно поиграть. Наша задача - следить за тем, чтобы они были в максимальной безопасности на игровой онлайн-площадке.

## Как рассказать детям о безопасности в Интернете

Теперь, когда вы узнали о некоторых потенциально опасных сайтах и ​​приложениях, самое время поговорить с детьми об интернете и безопасности в нем.

Вот несколько советов, чтобы ваша беседа прошла как можно более гладко:

### 1. Спросите ребенка, какие приложения и веб-сайты он использует

Попросите ребенка научить вас использовать и показать свои любимые приложения, игры или веб-сайты. Это поможет вам понять, как они работают, и выявить потенциальные риски с худшими приложениями для детей.

### 2. Обсудите с вашим ребенком все возможные проблемы

Если вы опасаетесь, что ребенок использует неподходящее для детей и подростков приложение или сайт, поделитесь с ним своим беспокойством. По возможности принимайте совместное с ребенком решение, чтобы он понимал причины, по которым не следует использовать то или иное приложение.

### 3. Будьте честны и откровенны с ребенком

Поговорите с ним о последствиях ненадлежащего использования технологий. Расскажите ему о кибербуллинге, взломе, [социальной инженерии](https://www.kaspersky.ru/resource-center/threats/how-to-avoid-social-engineering-attacks) и онлайн-ухаживаниях.

### 4. Убедите ребенка, что с вами всегда можно поделиться

Скажите ребенку, что вы не будете остро реагировать, если он сообщит вам о том, что видел в Интернете: например, неприятные комментарии, материалы сексуального характера или изображения насилия. Скажите также, что вы бы предпочли, чтобы он сообщил об этом вам, а не держал в себе. Покажите, как можно блокировать нежелательный контент или сообщать о нем.

### 5. Установите границы, но будьте реалистом

Устанавливаемые границы использования интернета должны зависеть от возраста ребенка и того, что приемлемо в вашей семье. Границы могут включать согласование следующих правил: сколько времени ребенок может проводить в сети и когда, не писать текстом вещи, которые он не сказал бы в лицо, не отправлять личные изображения, не сообщать вам пароль, чтобы вы могли проверить телефон ребенка.

### 6. Настройте родительский контроль

Настройте или пересмотрите параметры родительского контроля и интернет-фильтры. Родительский контроль предназначен для защиты детей от неприемлемого контента в интернете. Его можно использовать по-разному, например, чтобы обеспечить детям доступ только к соответствующему возрасту контенту, установить время использования устройства, отслеживать активность и не допустить передачу личной информации посторонним.

### 7. Убедитесь, что на устройстве ребенка установлены последние версии антивирусных программ

[Антивирусные программы](https://www.kaspersky.ru/antivirus) защищают устройства от внешних атак, находят и уничтожают потенциальные угрозы для системы и предупреждают о них. Новые вирусы появляются постоянно, и разработчики регулярно улучшают антивирусы, чтобы они оставались эффективными.

### 8. Убедитесь, что для ребенка установлены настройки максимальной конфиденциальности

Почти все приложения для социальных сетей имеют настраиваемые параметры конфиденциальности. Изучите их и вместе с ребенком настройте профили.

### 9. Используйте надежное решение кибербезопасности на устройствах детей

Решение [Kaspersky Safe Kids](https://www.kaspersky.ru/safe-kids) разработано специально для защиты детей в интернете. Оно состоит из двух приложений: одно нужно установить на устройство ребенка, второе – на смартфон родителя, чтобы просматривать отчеты и менять настройки. Встроенный родительский контроль даже позволяет управлять временем, которое дети проводят перед экраном на разных устройствах.

**WhatsApp**

**Что такое WhatsApp?**

Многие родители используют WhatsApp – популярное приложение для обмена сообщениями, позволяющее пользователям отправлять текст, видео, фото, выполнять звонки и общаться в видеочатах по всему миру.

**Безопасен ли WhatsApp для детей?**

* Дети и подростки могут общаться только с лицами из списка контактов на своем телефоне. Однако приложение позволяет делиться контентом, который может не соответствовать их возрасту. Это актуально, если друзья добавляют их в групповые чаты, и в конечном итоге у детей появляются контакты людей, с которыми они никогда не встречались лично.
* Следовательно, они смогут связаться с незнакомым человеком и оказаться незащищенными от контента, размещенного этим человеком.
* Пользователи не могут контролировать, кто добавляет их в групповой чат, но они всегда могут контролировать свое участие в чате: из чата можно выйти в любой момент.
* Рекомендуется рассказать ребенку, что если в групповом чате находятся незнакомые люди или люди, с которыми он чувствует себя неловко, следует выйти из чата и обсудить это с родителями.

**Tik Tok**

**Что такое Tik Tok?**

Tik Tok очень популярен среди детей и подростков; количество загрузок приложения [превышает 1,65 миллиарда](https://techcrunch.com/2020/01/16/44-of-tiktoks-all-time-downloads-were-in-2019-but-app-hasnt-figured-out-monetization/). Tik Tok позволяет пользователям создавать, публиковать и просматривать короткие музыкальные клипы, его еще называют «караоке цифровой эпохи». Возможность добавлять специальные эффекты к видео способствует творческому самовыражению.

**Безопасен ли Tik Tok для детей?**

* Когда в приложении регистрируются пользователи в возрасте от 13 до 15 лет, их учетные записи по умолчанию являются закрытыми. Это означает, что только друзья могут комментировать их видео. Только пользователи старше 16 лет могут вести прямые эфиры и обмениваться сообщениями, и только пользователи старше 18 лет могут покупать, отправлять и получать виртуальные подарки.
* Однако в приложении отсутствует возможность проверки возраста. Предполагается, что пользователи укажут фактическую дату рождения.
* Приложение поощряет активность, а многие пользователи желают продемонстрировать свои таланты, в результате чего мошенники с помощью лести и комплиментов могут [легко выйти на контакт с подростками](https://www.buzzfeednews.com/article/ryanhatesthis/tiktok-has-a-predator-problem-young-women-are-fighting-back).
* Некоторые родители выразили обеспокоенность по поводу использования ненормативной лексики в отдельных видео (хотя приложение запрещает пользователям искать нежелательный контент, например, по словам «секс» или «порно»).
* Родители также могут использовать для контроля ограниченный режим или режим семейной безопасности, позволяющий связать свою учетную запись с учетной записью ребенка и полностью контролировать настройки.