



**Муниципальное бюджетное учреждение  
дополнительного образования  
«ДЕТСКАЯ ШКОЛА ИСКУССТВ №7»  
городского округа Самара**

---

**443074, г. Самара, ул. Авроры, 117 тел. 264-94-81  
электронная почта: [artschool7@rambler.ru](mailto:artschool7@rambler.ru)**

# **Безопасность детей и подростков в сети интернет и мультимедийном пространстве**

Составил:  
педагог-организатор  
МБУ ДО «ДШИ №7» г.о. Самара  
Коршунов Иван Сергеевич

Самара 2021 г

## **Введение**

Безопасность в интернете и медиа пространстве в последнее время является неотъемлемой составляющей в вопросах, когда речь заходит о знакомстве детей с киберпространством. Уже в раннем возрасте ребенок знакомится с такими цифровыми устройствами как смартфон, планшет и компьютер, так как это становится важной составляющей в современном обществе. Всем известно, что интернет является кладезем полезной и важной информации, но одновременно с этим таит и немало опасностей, в особенности для неподготовленных людей, кем и являются дети и подростки.

Некоторые родители, чтобы оградить детей от опасного контента, запрещают им пользоваться интернетом, до тех пор, пока они не достигнут определенного возраста. Однако это не решает проблему в целом, так как общаясь со своими сверстниками ребенок или подросток также может получить временный доступ к такому контенту, с того же смартфона или планшета. Поэтому важно осознавать, что родители должны не только вести контроль за ребенком при использовании сети интернет и медиа ресурсов, но и формировать воспитание компьютерной грамотности во всемирной сети. На данный момент существует целый ряд различных программ, установив которые, можно обеспечить безопасность несовершеннолетних в сети.

Сейчас, когда информационные технологии общедоступны, со стороны правительства принимаются серьёзные меры по обеспечению безопасности всех граждан, обращающихся к ресурсам всемирной паутины – включая несовершеннолетних. Законодательство в сфере интернет-безопасности в разных странах мира может незначительно отличаться, но проблемы, с которыми оно борется, имеют сходное происхождение. В одних странах запрещается регистрация в социальных сетях с 13-ти летнего возраста, в других закрыт доступ к определенным ресурсам и порталам, в третьих интернет провайдеры обеспечивают строгий контроль безопасности сайтов и медиа контента на них.

Одной из основных причин возникновения таких правовых мер стала уязвимость детей дошкольного и младшего школьного возраста в сети интернет – ведь именно дети этих возрастных категорий становятся легкой добычей для разного рода интернет мошенников и преступников, которые посредством сети совершают сексуальные домогательства по отношению к несовершеннолетним, а также подвергаются унижению, втягиванию в незаконную деятельность, в процессе общения в сети, во время которого в доверие к ребёнку втирается незнакомый человек для использования его в своих целях.

Для этого стоит разобрать основные понятия угроз и их влияние, а в последствии и методы борьбы с данными опасностями, о которых поговорим далее.

### **Основные понятия**

Несмотря на то, что интернет предоставляет детям быстрый и удобный доступ к полезной информации, а также к развлекательным материалам, все же пользование всемирной сетью сопряжено с огромными рисками. Ниже мы познакомимся с наиболее распространенными из них.

**Нежелательный контент** – это различные материалы и страницы, в которых нет вирусов и вредоносного программного обеспечения, а сама информация представляет опасность.

Находясь в интернете, ребёнок может с легкостью натолкнуться на нежелательный контент, особенно если на устройстве не установлены специальные, ограничивающие данные материалы, программы. Чаще всего в роли таких материалов выступают сцены насилия, порнографии и другие материалы, вызывающие страх, ужас и панику у ребёнка, что может нанести вред его здоровью и развитию. В результате такого длительного воздействия психическое состояние детей серьёзно страдает.

**Интернет-хищники** – это личности использующие социальные сети, чаты, мессенджеры, интернет-форумы и другие социальные средства коммуникации для общения с детьми и подростками, с целью склонить их к незаконным действиям сексуального характера. Домогательства могут происходить как в пределах интернет-сервисов, так и «выходить в офлайн» - иногда интернет-хищники добиваются личной встречи с жертвой. Онлайн-преследования могут включать в себя отправку детям и подросткам непристойные сообщения, изображения, видео. Однако в первую очередь интернет-хищники пытаются наладить с жертвами доверительные отношения – порой выдавая себя за их сверстников.

Особая опасность состоит в том, что преступники способны без особого труда скрыть свою подлинную личность – это затрудняет их поиски в реальной жизни. Спрятавшись за фальшивой личиной, интернет-хищники, с помощью онлайн платформ – особенно часто это происходит в социальных сетях – склоняют детей к незаконным действиям, в том числе и сексуального характера.

**Интернет-преступность** – это преступность, связанная со сферой информационных технологий, целью которой является кража личной

информации, финансовых средств, незаконное присвоение информации, другое название этого термина киберпреступность.

Находясь в сети, ребёнок может стать жертвой преступника, даже не догадываясь об этом. Все это может привести к краже личной информации пользователя, включая имя, адрес, дату рождения, текущее местоположение и т. д. Но самое страшное, если для выхода в интернет ребёнок использует одно из устройств родителей, например, ноутбук – в этом случае может произойти похищение личных данных, которые в дальнейшем могут быть легко скомпрометированы.

**Интернет-запугивание** – использование личностями социальных сетей, чатов, мессенджеров, интернет-форумов и другие социальные средств общения с детьми и подростками с целью их запугивания, травли. Другое название этого термина Кибербуллинг.

Социальные сети образуют благоприятную среду для киберхулиганов, чье онлайн поведение несет в себе опасность. Риск подвергнуться травле в интернете сейчас очень высок, поэтому родителям нужно следить за тем, что происходит с их ребёнком в социальных сетях, а также объяснять, что он может поделиться с родителями любой проблемой, какой бы она ни была, особенно если ребёнок становится жертвой интернет-запугивания.

### **Способы обеспечения безопасности**

Рассмотрев несколько разных типов интернет угроз, с которыми дети и подростки могут столкнуться в интернете или сетевых медиа ресурсах, возникает вопрос о возможности противостоять этим опасностям. На данный момент таких способов очень много, к ним относятся антивирусы, VPN сервисы, программы слежения и мониторинга, которые позволяют родителям контролировать деятельность своих детей в интернете. Большинство этих программ общедоступно как в платном, так и бесплатном исполнении.

Начать стоит конечно с антивирусного программного обеспечения, так как именно оно на самых первоначальных этапах, помогает бороться с нежелательным контентом и киберпреступниками. Так как базы данных часто обновляются, они несут информацию о сайтах с непроверенным контентом, предотвращают попадание на устройство различного рода вредоносных программ, защищая тем самым устройство, которым пользуется ребенок или подросток, а также в дальнейшем предотвращая влияние пагубной информации в интернете на психику и здоровье ребенка.

На данный момент рынок предлагает широкий ряд антивирусного программного обеспечения, которое включает в себя инструменты для

защиты детей от угроз в сети. Примеры такого антивирусного обеспечения представлены ниже:

- Kaspersky Internet Security 2021
- ESET NOD32 Smart Security
- Dr.Web Security Space 12
- Norton Internet Security
- Trend Micro Internet Security
- McAfee Internet Security

Большинство этих антивирусных пакетов имеют приставку Internet Security, так как предоставляют более качественную защиту в сети интернет в отличие от своих упрощенных вариантов. Они блокируют сайты с запрещенным контентом, переходы по вредоносным ссылкам, предотвращают установку вредоносных программ из сети, так и с локальных источников. Таким образом установив уже данное ПО, мы получаем начальную защиту для ребенка от нежелательного контента и защиту устройства от возможных интернет преступлений.

Виртуальные частные сети или VPN что же это такое? Простыми словами «Виртуальная Частная Сеть» – это технология, позволяющая обеспечить безопасное сетевое соединение поверх небезопасной сети. С помощью VPN можно использовать Интернет без опасения, что интернет-преступники смогут определить местоположение пользователя и в дальнейшем попытаться произвести атаку с целью хищения личной информации. Данная технология в связи с высоким спросом сейчас очень популярная, примеры таких сервисов можно увидеть ниже:

- Express VPN;
- Tunnel Bear;
- Cyber Ghost;
- Hotspot Shield;
- Avira Phantom VPN.

Многие из тех антивирусных программ, перечисленных ранее, уже включают в себя VPN технологию, что позволяет пользоваться всеми преимуществами комплексной защиты, оберегая как свой компьютер, планшет, смартфон от вредоносных программ, так и ребенка от угроз интернет-преступников.

Ну и наконец можно перейти к одному из самых важных и значимых инструментов контроля и безопасности, в данном случае речь идет о приложениях родительского контроля. Это незаменимый инструмент, позволяющий родителям отслеживать активность ребёнка в Интернете и сетевом медиа пространстве. Используя данное ПО и сервисы, можно узнать, какие веб-сайты посещал ребёнок, какой контент он просматривал и какие приложения использовал. Программы, реализующие родительский контроль, становятся действительным залогом безопасности для всех, кто стремится обеспечить благополучие своих детей в эпоху Интернета. К одним из самых популярных приложений стоит отнести такие примеры как:

- Norton Family Parental Control;
- Kaspersky Safe Kids;
- K9 Web Protection;
- Qustodio Family Protection;
- KidLogger.

С их помощью можно ограничить время нахождения ребёнка в интернете, что увеличит количество времени для общения с друзьями и семьей, прогулок на свежем воздухе и занятий спортом. Кроме того, данные программы предоставляют родителям возможность блокировки определенных веб-сайтов, еще до того, как ребёнок обратится к ним – в том числе сайтов с играми и сайтов, содержащих порнографические материалы.

### **Рекомендации по детской интернет-безопасности**

В данном разделе мы рассмотрим некоторые советы, помогающие обеспечить высокий уровень безопасности для детей и подростков при использовании сети интернет.

С чего стоит начать? *В первую очередь* с правилами безопасности, потому что какие бы программы и сервисы мы не использовали, без надлежащего интернет воспитания невозможно построить защиту ребенка или подростка от внешнего информационного воздействия. Расскажите ребёнку об опасностях, с которыми он может столкнуться в сети, это исключительно важный момент. Родители не только должны досконально изучить вопрос безопасности детей в интернете, но и обучить самих детей правильному поведению в сети, чтобы исключить возможность возникновения опасных ситуаций.

*Второе.* Обязательно обсудите с ребёнком все проблемы, затронутые в этой статье, расскажите о существовании онлайн мошенниках, использующих вредоносные программы, интернет-преступности, интернет запугиванию, чтобы в дальнейшем ребенок был подготовлен к опасностям интернет сетей. Подобно обучению ребёнка правильно переходить улицу и не разговаривать с незнакомцами, по аналогии также требуется объяснить, что при неправильном использовании интернет может быть очень опасен.

*Третьим* и не менее значимым пунктом, следует показать ребёнку, что вы готовы всегда его выслушать. Чрезвычайно важно, чтобы ребёнок, подросток понимал – родители открыты для разговора, когда речь идет о безопасности в интернете. Если у ребёнка появляются проблемы, связанные со всемирной паутиной, он должен осознавать, что в любой момент может поделиться ими с родителями. В случае если ребёнок или подросток становится жертвой травли в интернете, родителям следует дать понять, что они всегда готовы помочь ему советом и поддержкой.

После первых воспитательных азов можно переходить к использованию безопасного ПО, антивирусных программ, инструментам родительского контроля, VPN сервисам.

Использование антивирусного ПО поможет обезопасить детей и подростков от сайтов, содержащих запрещенный и нежелательный контент, ненадежные программы, в том числе вредоносные программы, скрывающиеся мошенниками в компьютерных играх, подвергшихся взлому. Используйте инструменты для реализации родительского контроля гарантирующие родителям, что их ребёнок не получит доступа к вредоносному контенту или неподходящим, по мнению родителей, веб-сайтам, которые могут повлечь нарушение психического состояния.

Родительский контроль прост в установке. К примеру, встроенная функция в браузере Google Chrome позволяет ограничить доступ ребёнка к нежелательным веб-сайтам, например, к видео хостингу YouTube. После добавления сайта в так называемый «чёрный список», все попытки ребёнка перейти по этому адресу будут пресечены. Также к примеру установка приложения Kaspersky Safe Kids позволяет производить мониторинг использования смартфона или планшета ребенком, и также ограничивать доступ к нежелательному контенту, или ограничивать время препровождение в играх. Также стоит отметить и VPN сервисы, которые также позволяют отгородить детей от нежелательного контента в интернете. К тому же преимущество последних заключается в том, что их настройка предельно проста, а некоторые из них уже имеют встроенные шаблоны использования.

Также большинство провайдеров и операторов сети интернет предлагают данную опцию для семейного использования в своих тарифах.

Несмотря на то, что всемирная паутина – это отличный инструмент для детей и подростков, особенно с точки зрения доступа к образовательным ресурсам и развлечениям, при чрезмерном использовании интернет может затормозить развитие ребёнка. Чтобы избежать злоупотребления нахождением ребёнка в сети, важно ограничить время пользования цифровых устройств. Данная мера заставит его проводить больше времени в реальном мире с семьей и друзьями.

### **Заключение**

Всемирная паутина – это удивительный источник информации. Жизнь современного человека немыслима без интернета. Так как его платформы подвергаются постоянному развитию, никуда не деться от того, что большая часть детей будет взрослеть, используя интернет для обучения и развлечения. Именно поэтому с раннего возраста нужно обучить ребёнка правилам интернет-безопасности.

Разрешив ребёнку пользоваться интернетом, родители подвергают его множественным рискам. Тем не менее, правильное интернет воспитание, использование множество инструментов (VPN, родительский контроль, антивирусное программное обеспечение) и приложений, позволяет сформировать безопасную среду для детей и подростков при использовании информационных ресурсов. Помните, безопасность ребёнка в интернете на 90% зависит от его родителей.

Когда дети достигают определённого возраста – в частности речь идёт о подростках – их интересы довольно часто вступают в противоречие с установленными родителями правилами безопасности. Подростки стремятся быть более независимыми от родителей. Тем не менее, неограниченный доступ к сети интернет может стать настоящей проблемой. Такой нежелательный контент, как видео со сценами насилия, жестокие компьютерные игры, материалы с рейтингом 18+, порнографические изображения – притягивает подростков как магнит. Поэтому, даже предоставляя несовершеннолетним свободу действия в интернете, родители все равно могут и дальше использовать приложения, ограждающие их ребёнка от материалов нежелательного содержания.