

The background features a stylized globe with a blue and green color scheme. A grey spiderweb is superimposed over the globe. A laptop is positioned in the center, with its screen displaying a blue '@' symbol. Six cartoon children are depicted: a boy in a yellow shirt and blue pants is climbing the web on the left; a girl with long red hair in a green dress is sitting on the globe at the top; a girl in a pink dress is jumping on the right; a boy with glasses in a blue shirt is hanging from the web on the left; a boy in a green shirt and brown pants is hanging from the web at the bottom left; and two boys are hanging from the web at the bottom right. The overall theme is digital safety for children.

Безопасность детей в Интернет - пространстве

Ниязгулов Ильяс 8В г.Казань
Казанская Кадетская школа -
Интернат им. Б. К. Кузнецова



- Для обеспечения безопасности детей в интернете существует множество разнообразных инструментов: антивирусное программное обеспечение, VPNs (виртуальные частные сети) и приложения для реализации родительского контроля. Благодаря этим инструментам родители получают возможность контролировать деятельность их детей в сети, что обеспечивает разумное использование интернета ребёнком.



Антивирусное программное обеспечение

Пренебрегая антивирусными программами, вы подвергаете устройство вашего ребёнка риску. Данные программы предназначены для предотвращения совершаемыми киберпреступниками попыток взлома цифровых устройств – ноутбуков, планшетов, смартфонов и т. д.



Рынок предлагает широкий ряд антивирусного программного обеспечения, которое включает в себя инструменты для защиты детей от угроз в сети. Ниже представлены некоторые из основных поставщиков антивирусных программ:

Dr.Web Security Space 11
Kaspersky Internet Security
ESET NOD32 Smart Security
McAfee
TrendMicro
Symantec (Norton)



Большинство платформ
антивирусного программного
обеспечения предоставляют
собой эффективные
инструменты, блокирующие
доступ ребёнка к сайтам,
содержащим вредоносное ПО.
Используя антивирус
ESETNOD32 SmartSecurity
родители сами выбирают те
категории сайтов, к которым
несовершеннолетний будет
иметь доступ. Переход на все
остальные ресурсы, не
попадающие под данные
категории, будет заблокирован.



VPNs (виртуальные частные сети)

Что такое VPN? Простыми словами «Виртуальная Частная Сеть» – это технология, позволяющая обеспечить безопасное сетевое соединение поверх небезопасной сети. С помощью VPNs можно использовать Интернет не опасаясь, что киберпреступники смогут определить местоположение пользователя, а значит не смогут воспользоваться данной информацией для кибератаки. Ниже представлены несколько крупнейших VPN серверов :

ExpressVPN;
Hotspot Shield;
Windscribe;
TunnelBear;
Hide.me



Многие из тех
антивирусных программ,
перечисленных ранее,
уже включают в себя VPN
технологии, что
позволяет пользоваться
всеми преимуществами
комплексной защиты,
оберегая как свой
компьютер от
вредоносных программ,
так и ребенка от угроз
киберпреступников.



Приложения для реализации родительского контроля

Приложения родительского контроля – это незаменимый инструмент, позволяющий родителям отслеживать активность ребёнка в Интернете. Используя данные сервисы, можно узнать, какие веб-сайты посещал ребёнок, какой контент он просматривал и какие приложения использовал.



Приложения, реализующие родительский контроль, становятся действительным залогом безопасности для всех, кто стремится обеспечить благополучие своих детей в эпоху Интернета.

Ниже представлены лучшие приложения родительского контроля:

Где мои дети;
Kids360;
Norton Family Parental Control;
Screen Time;
KidControl;
mSpy;
KidLogger;
K9 Web Protection.



Где мои дети





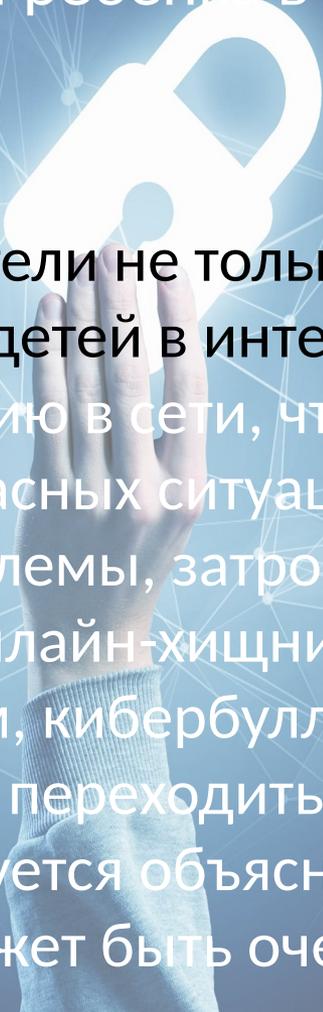
С их помощью можно ограничить время нахождения ребёнка в интернете, что увеличит количество времени для общения с друзьями и семьей, прогулок на свежем воздухе и занятий спортом. Кроме того, данные программы предоставляют родителям возможность блокировки определенных веб-сайтов, еще до того, как ребёнок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

Советы для родителей по детской интернет-безопасности

В данном разделе представлены советы, которые можно легко применить для обеспечения безопасности ребёнка в Интернете.

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. Обязательно обсудите с ребёнком все проблемы, затронутые в этой статье, расскажите о существовании онлайн-хищников, киберпреступности, вредоносных программ, кибербуллинга. Мало того, что нужно научить ребёнка правильно переходить улицу и не разговаривать с незнакомцами, также требуется объяснить, что при неправильном использовании интернет может быть очень опасен.



Покажите ребёнку, что готовы всегда его выслушать

Покажите ребёнку, что готовы всегда его выслушать

Чрезвычайно важно, чтобы ребёнок 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.



Если ребёнок становится жертвой травли в интернете, родителям следует дать понять, что они всегда готовы помочь ему советом и поддержкой.

Используйте инструменты для реализации родительского контроля

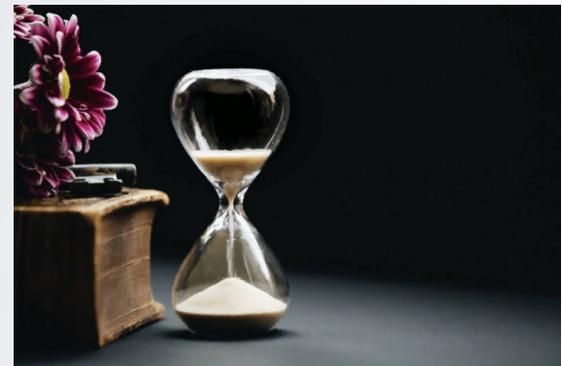
Родительский контроль – это комплекс мер, которые гарантируют родителям, что их ребёнок не получит доступа к вредоносному контенту или неподходящим, по мнению родителей, веб-сайтам, в том числе и к социальным сетям – Facebook, Twitter и ВКонтакте. Родительский контроль прост в установке. К примеру, встроенная функция в браузере GoogleChrome позволяет ограничить доступ ребёнка к нежелательным веб-сайтам, например, к видеохостингу YouTube.com. После добавления сайта в так называемый «чёрный список», все попытки ребёнка перейти по этому адресу будут пресечены.

Узнайте, какими приложениями пользуется ваш ребёнок, сколько времени он на это тратит, играет ли он в игры во время уроков. Смотрите статистику, определяйте точное местоположение и слушайте звук вокруг с помощью сервиса «Где мои дети».

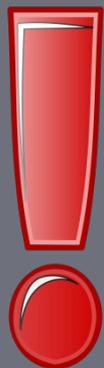


Ограничьте время использования устройств

Создается ощущение, что люди сутки напролёт готовы пользоваться услугами сети Интернет. Несмотря на то, что всемирная паутина – это отличный инструмент для детей, 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 ребёнка проводить больше времени в реальном мире с семьей и друзьями.



Используйте надежные пароли



Объясните ребёнку, что надёжные пароли способны повысить информационную безопасность в сети.

Поясните, что при регистрации на веб-сайте требуется придумать запоминающийся, но в то же время сложный пароль – это поможет снизить риск взлома учетной записи в Интернете.



Мошенничество в Интернете

Многие люди, в том числе дети, становятся жертвами безопасных на первый взгляд всплывающих окон и спам-сообщений, созданных и рассылаемых киберпреступниками. Эти всплывающие окна и спам-сообщения могут быть очень опасными и, вероятнее всего, приведут к заражению устройства компьютерным вирусом.



Покажите ребёнку отличительные признаки вредоносных программ, чтобы при встрече с ними в интернете он смог избежать проблем.

Дети и социальные сети

Социальная сеть, без сомнения, является одной из самых революционных технологий XXI века. Миллионы пользователей по всему миру выбирают социальные сети, такие как Facebook и ВКонтакте. Эти ресурсы показали себя эффективным инструментом для общения, создания онлайн-сообществ и продвижения бизнеса. Тем не менее, когда речь заходит о детях в социальных сетях, особенно если они только начинают знакомиться с ними, данные технологии таят в себе ловушки, о которых следует знать заранее.



Проблемы в социальных сетях



Как уже говорилось ранее, кибербуллинг получил широкое распространение в эру развития социальных сетей. Так как число случаев кибербуллинга в сети продолжает расти, нужно быть готовым, что любой ребёнок в Интернете может столкнуться с угрозой психологического насилия.



Помимо этого, нахождение ребёнка в социальных сетях в разы увеличивает риск атаки интернет-хищника. Преступные личности в целях маскировки очень часто используют фальшивые профили, напоминающие профиль ребёнка. Именно поэтому в момент знакомства с социальными сетями ребёнок должен быть предупрежден об опасности встречи с интернет-хищниками.

Ограничения по возрастным категориям

Родители должны сами решить в каком возрасте их ребёнок начнет пользоваться социальными сетями. У большинства социальных сетей для лиц младше 13 лет доступ к платформам и регистрация на них запрещены. Однако, некоторые родители, предпочитают дождаться пока их ребёнок достигнет определенного уровня зрелости, прежде чем ему разрешат ему пользоваться социальными сетями (Facebook, Twitter, VK и др.).

12+

16+

Контролируйте деятельность ребёнка онлайн

Если ребёнок пользуется социальными сетями, родители должны следить, чем он занимается в сети: какую информацию выкладывает в своём профиле, с кем общается, какие материалы читает и т.д. Отличным инструментом для этих целей могут стать приложения, реализующие родительский контроль – например, сервис «Где мои дети», позволяющий узнать, сколько времени ребёнок проводит, общаясь в социальных сетях и мессенджерах.

Интернет и дети подросткового возраста

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.

Поэтому, даже предоставляя несовершеннолетним свободу действия в интернете, родители все равно могут и дальше использовать приложения, ограждающие их ребёнка от материалов нежелательного содержания. В этом случае по-прежнему уместно использование различных инструментов, о которых говорилось ранее – в частности приложений и сервисов, реализующих родительский контроль. Данная мера позволит родителям обеспечить детям ту приватность в сети интернет, к которой они стремятся, и одновременно с этим избавит их от страха, что ребёнок натолкнется на нежелательный контент.



Такой нежелательный контент, как видео со сценами насилия, жестокие компьютерные игры, материалы с рейтингом 18+, порнографические изображения – притягивает подростков как магнит.

Безопасность детей в интернете:

ОСНОВНЫЕ ПОЛОЖЕНИЯ

Всемирная паутина – это удивительный источник информации. Жизнь современного человека немислима без интернета. Так как его платформы подвергаются постоянному развитию, никуда не деться от того, что большая часть детей будут 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, существует множество инструментов (VPN, родительский контроль, антивирусное программное обеспечение) и приложений, которые можно установить на устройство – например, приложение, ограничивающее по времени нахождение в сети – чтобы обезопасить ребёнка при работе в сети. Помните, что безопасность ребёнка в интернете на 90% зависит от его родителей.



Спасибо за внимание!

