«Родительский контроль»

Об информационно-технических способах защиты детей от вредоносных сайтов, игр, приложений, интернет-рисков и от негативного информационно-психологического воздействия

1. «Родительский контроль», реализованный операторами сотовой связи

- *Контроль за местонахождением ребенка*
- *Контроль за вызовами на/с телефона*
- *Включение/отключение Интернета*
- *Блокировка некоторых сайтов*

Подключается как сервис или приложение; платно

2. «Родительский контроль», реализованный в ОС Windows на ПК

- родители могут организовать работу ребенка за ПК (ограничение времени работы, запрет на включение после какого-то времени)
- запретить использование определенных программ или сайтов (блокирование инсталляции программ, запрет сайтов по ключевым словам)
- просматривать статистику активности ПК (все действия ребенка за ПК: какие программы запускал и сколько в них работал)

Работает в любой версии Windows, но для каждой есть свои особенности настройки; бесплатно

3. «Родительский контроль», реализованный в дополнительных программах под Windows на ПК

Помимо стандартных инструментов контроля Windows, из магазина Microsoft Store можно скачать и другие программы для организации детской работы за компьютером. Чаще всего их функция - ограничения работы в Интернете (контроль поиска информации)

ПРИМЕР: средства Windows Live, Wacky Safe, Kid Search, KidsControl; частично платные

3.1. Приложение Kaspersky Safe Kids
(для компьютеров, Андроида и Айфонов)

- Определение местонахождения ребенка на карте в режиме реального времени
- Установление безопасного периметра на карте и отправка уведомлений в случае выхода ребенка за его пределы
- Отправка уведомлений о низком уровне заряда батареи на устройстве ребенка
- Отслеживание звонков и SMS ребенка на устройстве Android
- Отчеты о публикациях ребенка в Facebook и ВКонтакте и изменениях в списке друзей
- Советы (уведомления-подсказки) профессионального психолога относительно онлайн-активности ребенка
- Блокирование доступа к нежелательным веб-сайтам и контенту

Частично платно; по отзывам – иногда «глючит»

4. Родительский контроль для мобильных телефонов и планшетов

4.1. Для iOS (Айфонов):

- Запрет на пользование различными сервисами и приложениями Apple (например, браузером Safari);
- возможность скрыть с устройства приложения «Камера», «FaceTime» (для осуществления звонков через интернет) и отключить голосовой ассистент Siri;
-можно заблокировать доступ к iTunes Store (позволяет приобретать музыку и фильмы) и iBooks Store (позволяет приобретать и скачивать книги), к профилям и публикациям музыкальных исполнителей в приложении «Музыка», установке и удалению программ из App Store, а также встроенным покупкам;
- возможность не запрещать использование приложений целиком, а ограничить потребляемый через них контент.

НО! Не позволяет устанавливать ограничения по времени использования устройства и приложений, блокировать устройство в определенный временной период (например, ночью) или удаленно. Нет функции определения местоположения ребенка.

4.2. Родительский контроль для Android-устройств

Возможности родительского контроля на Android более скудные и ограничиваются установкой возрастного рейтинга на скачиваемые приложения из Google Play.
Также имеется возможность запретить доступ к песням с ненормативным содержанием.

Однако у Google есть продвинутый сервис **Family Link** (ПРИЛОЖЕНИЕ), который позволяет:
- устанавливать время блокировки устройства, например на ночь, в том числе удаленно;
- устанавливать время использования устройства;
- получать статистику по использованию приложений;
- ограничивать нежелательный контент;
- получать рекомендации по полезному контенту;
- отслеживать местоположение ребенка;

Требуется скачать Приложение на родительский смартфон или установить настройки на сайте Google для аккаунта ребенка. Работает не на всех устройствах. Для детей до 13 лет. Частично платно.

Рейтинг Приложений Родительского контроля от Роскачества
(Роскачество – национальная система мониторинга, сравнительных испытаний и подтверждения качества товаров и услуг, учрежденная распоряжением Правительства РФ):

По критериям функциональности и безопасности лучшими приложениями для родительского контроля признаны:

•Android:
Kaspersky SafeKids (4,40 баллов),
Kidslox (4,37),
Mobile Fence Parental Control (4,10)

•iOS:
Kaspersky SafeKids (4,53 балла),
Kidslox (4,51),
встроенный родительский контроль iOS (4,20)

5. Сервис родительской опёки от Social Data Hub, который позволяет родителям «мониторить» своих детей в соцсетях

Платный сервис анализирует публикации, лайки, подписки и комментарии ребенка во всех социальных сетях, насколько активно он общается, меняется ли состав его друзей или поведение в соцсети.

В России сервис запускался в 2017 году с вызвавшим общественный резонанс слоганом «Лучше мы, чем ФСБ».

Владелец сервиса подчеркивает, что программа анализирует исключительно открытую информацию и не нарушает российское законодательство. Она не имеет доступа к личной переписке и гео-перемещению.

Чтобы подключить сервис, родителям надо зарегистрироваться на сайте компании, пройти проверку и подтверждение, что они подлинные родители. У родителей проверяется дата их регистрации в соцсети, «не чистил ли аккаунт, не удалял ли, не менял ли свою модель поведения». Также изучаются фотографии и публикации родителей, после чего потенциальных клиентов «пробивают» по базе судопроизводства. *Сервис вызывает споры.*

«Не ходите, дети, в Африку гулять» или этические аспекты «слежки» за детьми в интернете

- Эффективны ли категоричные запреты для детей? Запретный плод – сладок?
- На каждое действие есть свое противодействие?
-Доверяй, но проверяй?
-Самое главное – любыми средствами уберечь ребенка от потенциальной опасности?
-Вторжение во внутренний мир ребенка? Право на личную жизнь у ребенка?
-Если есть слежка, то нет доверия?
-Какой должна быть реакция родителей на полученную информацию о ребенке?..

Какие существуют интернет-риски для детей?

1. Контент-риски: материалы, содержащие вредоносную опасную, противозаконную, неэтичную, шокирующую информацию).
2. Коммуникационные риски:
- установление незнакомцем дружеских отношений с ребенком с целью растления, изнасилования;
- кибер-преследование (выманивание информации с целью запугивания, подражания, мошенничества, шантажа; хулиганство (интернет-троллинг); социальное бойкотирование);
- оказание злоумышленником на ребенка информационно-психологического воздействия (вовлечение в секты, в суицидальные игры, в экстремистскую и противозаконную деятельность, внушение).
3. Потребительские риски: кибер-мошенничество (причинение материального ущерба: хищение личной информации ребенка или его родителей (коды, пароли, номера банковских счетов, паспортные данные и др.).
4. Электронные риски: вредоносные программы (вирусы, черви, «трояны», шпионские программы, боты и др.), которые могут нанести вред компьютеру и нарушить конфиденциальность и целостность хранящейся в нем информации.

Решит ли проблему интернет-рисков для детей запрет на использование интернета?

Это тоже самое, что не разрешать ребёнку выходить на улицу, чтобы с ним ничего не случилось.
К тому же, готовы ли родители сами отказаться от смартфонов, компьютеров и, к примеру, любимого многими Инстаграма в качестве положительного примера?
«Двойная политика» приведёт к тому, что ребёнок перестанет доверять родителем, а в интернет будет выходить с телефона школьного друга или искать другие, менее безобидные способы.
А безапелляционно запрещая ребенку заводить аккаунт в соцсетях, родители только повысят притягательность этих социальных сетей для него, и ребёнок будет искать способы обойти данный запрет.

Нужно ли ограничивать пребывание ребёнка в интернете?

Безлимитное общение с ТВ, монитором ПК, планшетом, гаджетом, смартфоном приводит к негативным последствиям для здоровья. Для всех членов семьи. Разве удастся отобрать у ребёнка планшет, если сами родители не расстаются со смартфоном или ноутбуком? Полезно ввести правило, которое будет распространяться на всех членов семьи, например: в назначенный час вечером все выключают компьютеры и складывают свои гаджеты в определённое место, чтобы не брать их до самого утра.

Эта игра на честность, и кто-то может сжульничать, но такое правило будет работать действеннее прямого запрета.

Говорить ли с ребёнком об интернет-рисках и как, чтобы это было реально полезно?

Часто информация об интернет-угрозах в головах самих родителей очень общая, расплывчатая и неструктурированная. Дети плохо воспримут такую абстрактную информацию, даже если взрослым она покажется исчерпывающей.

Более действенным будет разговор, когда родитель приводит конкретные примеры, - и чем младше ребенок, тем больше должно быть таких примеров.

Однако надо учитывать, что такие примеры не должны нанести вред ребенку: не вызывать ненужный интерес, не пугать, не шокировать.

Полезно вместе с ребенком разбираться в теме, ведь родитель тоже знает не всё и так же может подвергнуться интернет-угрозе.

Упор на доверительные отношения и взаимодействие.

Использовать ли технические средства, которые помогут родителям сделать пребывание ребёнка в интернете безопасным?

Ключевая фраза: «сделать пребывание ребёнка в интернете безопасным». Именно этим и следует руководствоваться родителям, при использовании технических средств: защитить ребёнка от нежелательного контента. Учитывать возраст ребенка при подборе технических средств.

Смогут ли дети «обойти» программы родительского контроля?

Дети постарше могут предпринимать такие попытки: например, использовать сайт-анонимайзер.
НО! Большинство программ контроля можно настроить так, чтобы закрыть возможность пользоваться такими сайтами.
Другой вариант – попытки ребенка подобрать пароль к настройкам программы: обычно это не очень сложно, если родители не отнеслись к выбору пароля серьёзно.
НО! Такие «военные действия» – сигнал неблагополучия в отношениях с ребенком.
Всегда полезнее объяснить ребёнку, что в интернете ему может попасться неприятная и страшная информация, он может увидеть ее случайно. Рассказать, что поставлена специальная программа, которая защищает ребенка, а не следит за ним.
Важно помнить, что чем больше доверия в отношениях, тем меньше поводов для беспокойства и фильтров в программах родительского контроля.

Запрещать ли ребенку социальные сети?

Запрещать - не выход.
Ограничивать – нужно.
Не ультиматум, а договоренности.
Предупредить о настройках родительского контроля, например: что в часы, когда время делать уроки, - социальные сети будут недоступны, и что сайты с сомнительным содержимым не будут открываться совсем.
Не стоит нарушать личное пространство ребёнка, читать его переписку и явно за ним шпионить.
Чтобы быть в курсе происходящего с ребёнком в соцсетях, и не только в них, - надо стать его другом, и реальным, и виртуальным.
Следует вести себя на страничках своего ребёнка как взрослая личность со взрослой личностью: лишнего не писать и не выкладывать и не «лайкать» всё подряд.
Полезно научить ребёнка здоровому сомнению: задавать наводящие вопросы в переписке с виртуальными знакомыми, не принимать всё на верну, не встречаться в реальности с новыми знакомыми из сети, не предупредив об этом взрослых, назначать встречи только в общественных местах, не сообщать свои личные данные и контактную информацию незнакомым людям, сделать свои странички в соцсетях закрытыми, установить настройки приватности, это минимизирует вероятность контактов с нежелательными персонами.
Нужно «грамотно» рассказать об опасностях и предупредите о последствиях.

Когда родителям надо бить тревогу?

Ребёнок, попавший под чужое влияние или затянутый в секту, МЕНЯЕТСЯ.
Но делает он это не за один день.
Для того чтобы заметить эти опасные перемены, нужно быть в постоянном контакте с ребенком, быть с ним по-настоящему близкими людьми: только тогда можно обратить внимание на незначительные перемены в его настроении.
Риск есть тогда, когда общение родителей с ребёнком происходит формально, а интерес они проявляют только к его учёбе и дисциплине.
Если родитель, к примеру, затрудняется назвать три вещи, события или ситуации, которые произвели впечатление на его ребёнка на прошлой неделе, - значит, в семейных отношениях нужно что-то пересмотреть.
Когда у родителя есть подозрения, что с ребёнком что-то не так, то для начала надо подтвердить или опровергнуть свои догадки: больше общаться с ребенком, задавать осторожные вопросы, не обвинять ни в чем и не уличать, особенно, если нет уверенности.
В случае необходимости надо обращаться с проблемами к специалистам.

КОНТАКТЫ

Куценко Валентина Александровна,
педагог-психолог
bd408@mail.ru

Материалы подготовлены
с использованием информации
из открытых источников в сети интернет