

## Предлагаем вам инструкцию по начальным азам Безопасности в Интернете.

Изучите технологию пользования интернетом

Используйте онлайн инструменты родительского контроля;

Включите ограничения в настройках конфиденциальности в интернет-браузере;

Выучите термины технологии и жаргон ребенка – юного интернетчика.

Контролируйте онлайн деятельность. Тоже будьте активным пользователем!

- Следите за ним на всех аккаунтах в социальных сетях; однако будьте внимательны и не дайте этому процессу перерасти в репрессивный контроль, потому что так ребенок будет стремиться «скрыться».
- «Подружитесь» в социальных сетях, ставьте оценки на его публикации, а если видите что-то, что вас беспокоит, поговорите с ним аккуратно, с глазу на глаз. Скажите ему, что вас беспокоит и почему;
- Интересуйтесь его виртуальными друзьями, с кем и куда ребенок ходит;
- Поставьте компьютер в пределах видимости (гостиная, кухня).
- Учите ребенка ответственности в онлайн
- Быть вежливым в онлайн, также, как и в реальной жизни – в школе, во дворе или на игровой площадке;
- Не говорить имя, адрес или другие личные данные чужим людям;
- Не отвечать чужим людям, также как он не разговаривает с чужими людьми на улице.

Покажите ему, что вам можно доверять. Если происходит что-то плохое, не критикуйте, а слушайте. Он должен знать, что может обращаться каждый раз когда почувствует в этом необходимость;

Помогите ему пройти этап стыда и стеснения.

Говорите ему как можно чаще, что вы доверяете ему.

Сообщайте о случаях подозрения или насилия на <https://siguronline.md/> или в полицию – 112.

**Детей нужно направлять, они должны понимать это и учиться пользоваться интернетом с ответственностью.**

Регулярно разговаривайте с ними о том, как они должны обеспечивать свою безопасность в онлайн.

Спрашивайте ребенка о том, что он думает о рисках или моделях поведения, похожих на риски в реальной жизни, например, домогательство. Поэтому лучше объяснить ребенку это, прежде чем что-то случится.

Этот процесс потребует времени, усилий и большого терпения со стороны родителей.

Интернет, при рациональном использовании, полезен для обучения или конструктивного проведения свободного времени.

Если ребенку запретить доступ к интернету, он будет скрываться или обманывать, он найдет другие способы воспользоваться интернетом.

## **С ребенком нужно обсуждать правила поведения в онлайн, чтобы он понимал их суть**

Ознакомьтесь с технологией. В силу своего возраста, дети более уязвимы: они доверчивы и не имеют жизненного опыта.

Интернет не создавал людей, совершающих насилие над детьми, но он облегчил способы установления контакта с ними.

**Настройки, фильтры содержания и программы родительского контроля помогают создать более безопасную среду для детей в онлайн, но только вместе с беседами об онлайн безопасности и правилах поведения в онлайн.**

Для того чтобы защитить ребенка от неуместной информации в интернете, опасных сайтов и вредоносных программ, активируйте настройки конфиденциальности, антивирусную программу, фильтр содержания в поисковых системах, Youtube, магазинах приложений и играх.

Установите комплексную программу родительского контроля для мониторинга деятельности ребенка в интернете и установите пределы времени, проводимого перед экраном.

Предлагайте ребенку помощь каждый раз, когда у него возникает проблема

Вы предоставляете ребенку доступ к Интернету, и хорошо убедиться, что он может использовать ответственно устройства, к которым у него есть доступ. Найдите время для того, чтобы его выслушать, не обвиняйте его и не критикуйте, если что-то происходит. Поддержите его и говорите, что доверяете ему. не публикуйте никаких фотографий или информации о ребенке

Старайтесь не публиковать изображения своего ребенка в ванной или любые другие фотографии, где он изображен частично или полностью раздетым. При описании фотографий не используйте уменьшительно-ласкательные слова или прозвища, потому что потом это могут использовать его коллеги из школы и ставить его в неудобные ситуации. Изображения с ребенком в школе, в которой он учится, или фотографии из лагеря, в котором он находится, в сочетании с полным именем, увеличивают риск того, что кто-то воспользуется этой информацией и нанесет вред.

## **Защита личных данных**

Вы беспокоитесь о том, что ваш ребенок публикует в интернете? Ваша обеспокоенность полностью обоснована.

Часто дети неосознанно раскрывают слишком многое в интернете.

Например, они могут невольно раскрыть данные личного характера о себе или родителях: номер телефона, домашний адрес, школу, в которой учатся, данные из удостоверения личности родителей, включая комбинацию чисел домашней сигнализации.

### ***Что такое личные данные?***

Личные данные – это данные человека, которые используются для его идентификации.

Они носят частный характер: имя и фамилия, личный цифровой код, дата рождения, физический или электронный адрес, номера телефонов, национальность, язык, пол, банковский счет, отпечатки пальцев, запись голоса, фотографии, IP адрес, школа и класс, распорядок семьи и т.д. Личные данные позволяют определить человека либо напрямую, либо путем объединения нескольких элементов информации.

Говорите с детьми о рисках

Родители учат детей с малого возраста не говорить слишком много незнакомым о том, что они делают, как делают, что у них есть и чего нет, чего хотят в подарок, куда едут, с кем и когда, не говорить незнакомыми на улице, быть внимательными, когда переходят улицу, не принимать подарки и т.д.

***В интернете – так же, как и в реальной жизни, нужно помнить о тех же правилах безопасности.***

В мире, где информация приобретает все большую ценность, личные данные становятся разменной монетой, особенно в социальных сетях. Загруженные изображения с различных сайтов или социальных сетей могут быть использованы, а если они содержат четкие элементы, определяющие домашний адрес или распорядок семьи, вся семья может оказаться под угрозой.

Например, опубликование фотографии или текстового сообщения о том, что семья в отпуске, может использоваться злоумышленниками для взлома дома.

Учите детей проверять политику конфиденциальности веб-страниц, на которые они заходят.

Также учите их не сохранять личные данные в навигаторе. Объясните детям причины таких мер предосторожности.

### ***Личная информация и фотографии детей в интернете***

Очевидно, что никто не согласится раскрыть свои личные данные незнакомым людям или сделать их общественным достоянием.

И дети тоже не согласились бы на это. Иными словами, все согласятся с тем, что никто не выйдет на улицу с альбомом фотографий или записями о личной жизни на улицу. Но, находясь перед мониторами, многие подростки в своих действиях переживают чувство иллюзорного одиночества – «ну я же дома, в безопасности, а не на улице», и поэтому легко соглашается предоставлять данные о своей личности или семье, чтобы быстро создать электронный адрес, чтобы поучаствовать в онлайн конкурсе или получить подарок, обещанный в онлайн объявлении.

Также, онлайн опубликование фотографий, сделанных на телефон или цифровой камерой, - процесс простой и быстрый.

Однако вам нужно знать, что, если вы публикуете фотографию в интернете, очень сложно предотвратить ее распространение, изменение или последующее использование в различных контекстах. Копии этих фотографий окажутся в нескольких местах и будет сложно стереть их все. Учите детей думать дважды, прежде чем опубликовывать личные данные.

### ***Учите ребенка:***

Быть внимательным, когда выбирает имя пользователя. Лучше не указывать полное имя и не ставить непристойные имена;

Не открывать для общего просмотра и не раскрывать в переписке в онлайн с незнакомыми людьми личную информацию;

Не давать никому пароли доступа к личным аккаунтам и часто их менять. Использовать разные пароли для различных аккаунтов, чтобы в случае, если аккаунт взломают, можно было восстановить другие аккаунты;

Понимать и избегать риски заражения используемых устройств вирусами;

Думать и читать прежде чем нажимать «ОК», «Согласен» или «Принимаю» на баннерной рекламе или неожиданно всплывающих окнах;

Менять пароли доступа ко всем используемым службам онлайн, таким как электронная почта, социальные сети и т.д., если их взламывают.

Важно объяснять важность этих мер предосторожности, чтобы дети лучше это понимали и с большей осознанностью соблюдали их.

Также говорите им, что они могут обратиться к вам каждый раз, когда сталкиваются с определенными сложностями или неприятными ситуациями в онлайн.

## **ПРОГРАММЫ ДЛЯ РОДИТЕЛЬСКОГО КОНТРОЛЯ НА КОМПЬЮТЕРЕ**

Родительский контроль компьютера — это набор программ и действий, который направлен на организацию или запрет использования детьми компьютерного времени, доступа к играм или другим программам, и самое главное — для избежания просмотра сайтов с “недетским” содержанием. Программы родительского контроля позволяют взрослым ограничивать контент, который смотрят и читают дети в интернете. Также можно легко распоряжаться временем, проводимым за компьютером. А еще несложно посмотреть, чем занимался ребёнок в ваше отсутствие в интернете. Простые примеры: после настройки родительского контроля компьютер сына или дочери будет включаться только после 6 вечера; игры будут доступны до 10 часов ночи; ни один сайт, содержащий в названии набор букв (s)\*ex или por\*(n), не будет открываться. Родительский контроль можно обеспечить как внешними программами, так и средствами операционных систем. Кстати, одним из самых полезных нововведений Windows как раз и считается наличие весьма гибких инструментов осуществления родительского контроля.

Родительский контроль скачать бесплатно вполне возможно, существуют хорошие некоммерческие программы, и зачастую многим пользователям достаточно уже встроенных в Windows инструментов. Перед обзором программ и настроек родительского контроля, дадим несколько советов. Конечно, это не программа родительский контроль, но может принести больший эффект, чем все ограничения и настройки. Первый шаг для того, чтобы сделать компьютер по-настоящему полезным для ребёнка: выбирайте игры и программы, соответствующие возрасту. Школьникам интересны прежде всего видеоигры (включая онлайн-развлечения), но не меньше их можно увлечь рисованием, презентациями, азами программирования, обработкой видеороликов, необычными функциями “скучных” текстовых редакторов, написанием текстов на интересующих их форумах и блогах. Детям будет приятно поиграть вместе с родителями, или чтобы взрослые смотрели на игру и обсуждали острые моменты. Если вы играете сами, то поболтайте о настройках игры, о её секретах, о прохождении, о функциях программ, которые удивляют и вас.

Чтобы включить Родительский контроль в Windows, нужно перейти в одноименный пункт Панели управления (через меню Пуск). Здесь выбираем профиль пользователя, в котором работает ваш ребёнок, именно на него мы сейчас и настроим ограничения, если у вас один профиль, то вам нужно создать специальный профиль (учётную запись) для ребёнка.

Сначала необходимо убедиться, что профиль ребёнка — обычный, а не администраторский. Для этого зайдите в Панель управления и выберите соответствующий профиль пользователя.

Создайте профиль, отличный от основного, задав основному пароль доступа, Дайте профилю название. Два профиля Windows - один для вас с паролем доступа, другой детский с ограничениями и работающим родительским контролем

Включите для новой учётной записи родительский контроль

Самое простое здесь это управление временем. Лёгкий интерфейс сразу предлагает задать время, когда ребёнок может войти в операционную систему (т.е. начать работу за компьютером). Можно настроить

расписание работы по дням недели. Система автоматически отключится, сохранив все данные, если ребёнок засиделся за клавиатурой.

Вместе с полезной для ребенка информацией в интернете его поджидают далеко не виртуальные опасности. Злоумышленники в социальных сетях, шок-контент и неприемлемое содержимое на сайтах, пропаганда насилия и наркотиков — все это может навредить ребенку. Родительский контроль на компьютере предназначен, чтобы ограничить доступ детей в интернет и оградить их от опасности.

Способов, как сделать родительский контроль на компьютере, довольно много. Самый простой из них — использовать встроенную функцию родительского контроля на компьютере в программах Windows. С ее помощью можно создать черный список сайтов, на которые ребенку будет закрыт доступ, или белый список. От черного он отличается тем, что позволяет заходить только на указанные в перечне сайты, блокируя при этом все остальные.

Настройки также позволяют обеспечить родительский контроль по времени на компьютере. Вы можете задать то, сколько ребенок будет работать с интернетом или определенным сайтом, настроить доступ в зависимости от времени и дня недели. Включить родительский контроль на компьютере можно через панель задач во всех версиях Windows, начиная с Vista.

Еще одним вариантом, как поставить родительский контроль на компьютер, является использование похожих функций в браузерах. Самые популярные — Opera и Google Chrome — имеют возможность включения родительского контроля над компьютером прямо в своих опциях. Расширить возможности можно при помощи установки дополнений, а в Mozilla Firefox это единственная возможность заблокировать ребенку доступ к нежелательным сайтам.

Интернет может сослужить как хорошую, так и плохую службу вашему ребенку. С одной стороны, это универсальное средство для развлечения и учебы. Множество полезных и интересных материалов развивают малыша, прививают ему любовь к чтению и помогают ему познавать мир. С другой стороны, в сети легко наткнуться на грубость, пропаганду наркотиков и шокирующие материалы, вредные для психики ребенка. Из этого появляется вопрос — как заблокировать нежелательные сайты в браузере, чтобы ребенок избежал опасности, сидя за компьютером? Самым простым способом является изменение файла hosts, который находится в системной папке Windows. Прописывая адрес локалхоста (127.0.0.1) напротив адреса нежелательного сайта, вы заблокируете к нему доступ, как только сохраните изменения в данном файле. Чтобы узнать, как заблокировать веб-сайт в браузере Google Chrome, необходимо покопаться в его настройках. При создании нового профиля, которым будет пользоваться ребенок, нужно отметить его как «контролируемый», и через дальнейшие настройки вы сможете легко добавлять нежелательные сайты в черный список, а также отслеживать историю посещения за день.

Альтернативой этому является бесплатное расширение BlockSite в магазине Google. Меню программы предоставляет большой выбор фильтров и настроек, а также систему паролей на блокировку, чтоб ребенок не смог изменить их самостоятельно. Если вы ищете способ, как заблокировать нежелательные сайты в других браузерах, то вряд ли найдете что-то новое. В Opera имеется возможность заблокировать нежелательное содержимое при помощи настроек, а Firefox — исключительно через дополнения вроде FoxFilter.

## **Time Boss — нужная программа для родительского контроля.**

Есть все нужные вам функции для ограничения времени, которое ваш ребенок проводит за компьютером. Time Boss защищен от всех попыток ребенка отключить программу. Первая версия была написана в 2005 году, с тех пор программа родительского контроля Time Boss развилась в успешный программный продукт с сотнями довольных пользователей в 54х странах мира. Программа ограничения времени работы на компьютере **Time Boss** создана чтобы дать родителям возможность ограничить время, которое наши дети проводят играя в компьютерные игры или сидя в интернете. **Time Boss** имеет простой дружелюбный интерфейс с многоязычной поддержкой, множество полезных, выверенных годами функций, использует защиту паролем (по умолчанию пароль **123**) и, по желанию, ведет журнал компьютерных событий, журнал скриншотов и полную статистику использования Вашего компьютера (какой пользователь, когда и что делал пока вы отсутствовали).

<http://nicekit.ru/parental-control/time-boss.php>