



ПАМЯТКА РОДИТЕЛЯМ ДЕТИ ЗА КОМПЬЮТЕРОМ

Автономная некоммерческая организация «Центр защиты детей от Интернет-угроз» (далее - «Центр») предостерегает о том, что несовершеннолетние наиболее подвержены опасностям сети «Интернет», а родители несут ответственность за своих детей.

Наш проект является социально-ориентированным. Мы крайне озабочены обстановкой в Интернет-пространстве.

Настоящая памятка поможет родителям самостоятельно настроить компьютер ребенка.

Подробности Вы можете найти на Интернет-сайтах Центра, разработчиков операционных систем и программного обеспечения.

У РЕБЕНКА КОМПЬЮТЕР. КАК ОБЕСПЕЧИТЬ КОМФОРТ И БЕЗОПАСНОСТЬ?

Компьютеры, ноутбуки, нетбуки (далее - «ПК») в находятся в личном пользовании практически всех детей. Как создать комфортные и относительно безопасные условия для работы ребенка на ПК, не прибегая к чьей-либо помощи?



ШАГ № 1. ПРАВИЛЬНОЕ РАСПОЛОЖЕНИЕ ПК

Компьютер должен располагаться таким образом, чтобы обеспечивалась правильная осанка, расположение кистей рук, движений головы. Не позволяйте ребенку проводить много времени с ноутбуком в положениях полусидя и лёжа.

Важными факторами расположения являются достаточность рабочего пространства и освещения. Вместе с тем, освещение не должно быть избыточным и создавать бликов/пятен на экране монитора.

ШАГ № 2. ВЫБОР ОПЕРАЦИОННОЙ СИСТЕМЫ

Операционная система (далее - «ОС») является основой и «двигателем» любого компьютера. Правильный выбор и настройка ОС помогут ребенку комфортно «общаться» с компьютерной техникой!

ОС, которыми пользуются дети:

- Семейство Microsoft Windows.
- Основанные на ядре LINUX - «Ubuntu», «Fedora», «Debian» и пр. (бесплатные).
- ОС компании Apple - «OS X» («MacOS»).

Важно, чтобы ОС была легальной. Это означает, что она официально приобретена либо предустановлена производителем ПК.

Большинство компьютеров и ноутбуков таких производителей, как HP, Packard Bell, Kraftway, Samsung и пр., уже готовы к работе «из коробки».

Не стоит размениваться на пиратские «сборки», которые легко можно найти в Интернете.

Недостатки «пиратских» ОС:

-Вы нарушаете авторские права разработчика ОС уже на стадии установки системы.

-Вы лишены техподдержки, не во всех «пиратках» возможно получать обновления безопасности.

-Система может быть внезапно деактивирована и работа в ней станет невозможной.

-ОС может часто зависать, работать некорректно.

-Пиратские сборки разрабатываются сообществами хакеров, которые оставляют «лазейки» для вирусов (так называемые БэкДоры). Будьте готовы к тому, что компьютер будет постоянно заражаться вредоносными компьютерными программами несмотря на наличие установленных антивирусов.

Также, получили распространения пиратские модификации ОС компании Apple под названием «Hackintosh».

В случае, если при покупке компьютера ОС не предустановлена, то рекомендуем её официально приобрести.

ОС приобретается «на всю жизнь», как и двигатель для автомобиля.

Бесплатные решения ОС на базе LINUX не привычны рядовым пользователям, но заслуживают внимания. Однако, с установкой и настройкой данной ОС придется повозиться и не все Windows-приложения удастся на ней запустить. Вместе с тем, в данных ОС удобно работать, они имеют больше просторов для навыков программирования и практически неуязвимы вредоносным программам.



ШАГ № 3. АНТИВИРУСНАЯ ЗАЩИТА

Важным этапом настройки компьютера ребенка является обеспечение надлежащей антивирусной безопасности.

Большинство антивирусных компаний предлагают бесплатные утилиты очистки и «загрузочные диски лечения».

Антивирусные программные продукты бывают платные, бесплатные, условно-бесплатные (ограниченный период бесплатного действия) и могут включать следующие компоненты защиты: **файловый антивирус, блокирование сетевых/внешних вторжений и атак (Firewall), обнаружение иных угроз, не отнесенных к категории вирусов и троянов (руткиты и пр.), эвристический анализатор и иные решения.**

Наиболее «продвинутое» решение антивирусных компаний включают в себя несколько компонентов защиты одновременно, а также необходимый родителям «бонус» - **систему родительского контроля.**

Возможен вариант одновременного использования решений различных разработчиков (например, антивирус+firewall) при отсутствии конфликта программ.

После установки антивирусного ПО, его необходимо настроить в соответствии с рекомендациями разработчика и Вашими требованиями. Помните, что установка антивирусного ПО, даже очень дорогостоящего, полностью не оградит компьютер от заражения.

Регулярно используйте антивирусы других разработчиков. Контролируйте обновляемость антивирусных баз. «Чистота» компьютера зависит от разумности и избирательности пользования Интернет-ресурсами, а также соблюдения правил Интернет-безопасности.

В случае скачивания антивирусных программных продуктов из непроверенных источников, Вы рискуете стать жертвой лжеантивируса, который будет только создавать видимость работы и выполнять противоположную функцию - заражение компьютера.



ШАГ № 4. СОЗДАНИЕ ДЛЯ РЕБЕНКА ОТДЕЛЬНОЙ УЧЕТНОЙ ЗАПИСИ В ОС

Итак, у ребенка установлена полноценная операционная система, чистая от вирусов и других нежелательных программ.

Учетная запись, которая создана при установке ОС является **Администраторской**, в нашем случае - **Родительской**. Вход в данную учетную запись должен быть защищен надежным паролем. Учетная запись ребенка будет пользовательской или **«Локальной»**, а в нашем случае - **«Детской»**.

«Детская» учетная запись создается, при входе в «Настройки», «Панель управления», а затем в «Учетные записи пользователей».

Далее надо выбрать тип учетной записи (в нашем случае - «Ребенок») и нажать кнопку «Создать учетную запись». На значок входа в учетную запись, можно установить фотографию ребенка, что будет приятным и интуитивно понятным для него моментом. Затем можно задать ограничения работы с компьютером. Важным плюсом является то, что ребенок не сможет без вас запустить файл и установить новую игру, пока Вы не введете пароль администратора. **Приучайте ребенка к тому, что новые игры и программы будут устанавливаться совместно с родителями!**

В различных версиях операционной системы «Microsoft Windows» создание и настройка учетной записи осуществляется с некоторыми особенностями.



ШАГ № 5. ИСПОЛЬЗОВАНИЕ ДОПОЛНИТЕЛЬНЫХ СРЕДСТВ РОДИТЕЛЬСКОГО КОНТРОЛЯ

Множество компаний предлагают дополнительное программное обеспечение, расширяющее возможности ограничений и контроля, заложенные в ОС путем:

-**запрета поиска по ключевым фразам.** Если ребенок наберет в Яндексe и Google запретное слово, то не сможет найти что ищет, а родителю возможно поступит об этом информация. Помните, что ребенок может использовать «не односложные» запросы.

-**ограничения доступа к потенциально опасным и нежелательным сайтам.** Вместе с тем, ни один разработчик программ не сможет объять миллиарды страниц сети Интернет и изучить их на предмет опасности и нежелательности.

-**отправки родителям подробных отчетов.** Помните, что Вам потребуется много свободного времени, чтобы данные отчеты изучить.

Для детей дошкольного возраста целесообразно использование решений, которые открывают доступ только к проверенным детскими сайтами и запрещают всё остальное. К таковым относятся, например, детский браузер «Гоголь», проект «ВебЛандия». **Эффективность работы данных решений зависит от правильности настройки рабочей среды.**

Помните, что ни одно программное средство не обеспечивает надлежащего контроля социальных сетей, средств обмена сообщениями, онлайн-игр и чатов! Мы можем обеспечить надлежащую настройку ПК и усиленный контроль ребенка. Обращайтесь к нашим специалистам!

Контакты Центра:

**390000, Рязань, Маяковского ул., 57, оф. Н13.
тел. (920) 966-65-15, e-mail: child-security@ro.ru
Интернет-сайт: www.child-security.net, также можете найти нас в социальных сетях.**