## 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 Яндексе 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 «Гогуль», 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!

Для консультаций по вопросам детской компьютерной безопасности обращайтесь к специалистам «Центра защиты детей от интернет-угроз»

**Контакты Центра:**
390000, Рязань, Маяковского ул., 57, оф. Н13.
тел.: 8 (920) 966-65-15,
**e-mail:** info@child-security.net
**Интернет-сайт:** www.child-security.net

## ЧЕМ ОПАСЕН ИНТЕРНЕТ ДЛЯ НАШИХ ДЕТЕЙ?

В «облаке» Интернет содержится огромный массив информации, подавляющая часть которой наносит вред здоровью, а также физическому, психическому, духовному и нравственному развитию детей. Кроме того, в Сети промышляют педофилы, мошенники, кибербуллеры, сектанты и иные злоумышленники, которые находят детей в Сети, а затем под различными предлогами вступают с ними в переписку и личный контакт.

Дети, по своей неопытности, не способны распознать опасность, а любознательность детей делает их крайне уязвимыми в интернет-пространстве.

Анонимность сети Интернет позволяет злоумышленникам и детям маскироваться в потоке информации и в переписке, что уже делает данную Сеть опасной.

Таким образом, опасности сети Интернет можно разделить на 3 основные категории:

1. Информация, которую ребенок просматривает самостоятельно, находясь в Интернет-пространстве.

2. Противоправные действия ребенка.

3. Действия Интернет-злоумышленников.

В последнее время, наиболее опасными для детей являются: педофилы. сектанты, интернет-аферисты, кибербуллеры и современные преступные сообщества.

По данным анонимных опросов, около половины школьников сталкивались с кибербуллингом и иными угрозами, не ставя в известность своих родителей.

При помощи Интернета, школьники вовлекаются в современные организованные группировки, например, хакеров, троллей и становятся участниками информационных войн. И это далеко не все опасности и неприятности, с которыми сталкиваются дети в сети Интернет!

## Как защитить ребенка?

Многие считают, что лучшей защитой является полный запрет на пользование Интернетом. Данный способ эффективен, но в современном мире неактуален, потому как Интернет общедоступен, а запрет может спровоцировать обиду и социальную деформацию ребенка. Эффективными мерами защиты являются интернет-воспитание, открытый диалог между родителями, педагогами, детьми и нашими специалистами, а также надлежащий контроль.

**МЫ РЕКОМЕНДУЕМ:**

1. Добиться у ребенка полного доверия и диалога по вопросам интернет-безопасности.

2. Установить с ребенком «правила» работы с компьютером, время работы, определить ресурсы, которые можно и нужно посещать. Объяснить, что Интернет, в первую очередь, является средством развития и обучения, и только второстепенно — средством развлечений и общения. Договориться, что новые игры и программы будут устанавливаться совместно с родителями.

3. Ограничить Интернет на смартфонах и планшетах, потому как мобильный Интернет позволяет бесконтрольно и постоянно общаться в соцсетях, отвлекает от учёбы и повседневных дел, а также развивает интернет-зависимость!

4. Запретить общение с неизвестными людьми.

5. Запретить ребенку пользоваться некоторыми видами ресурсов и программ, например онлайн-казино, жестокими играми и пр.

6. Настроить операционную систему, создать ребенку отдельную учетную запись, ввести различные ограничения.

7. Контролировать работу ребенка с компьютером и портативными устройствами, в частности, при помощи средств родительского контроля. При этом, ребенку нужно объяснить, что вы это делаете для того, чтобы предотвратить опасности, и что на это имеете полное право.

# ПАМЯТКА РОДИТЕЛЯМ

## Чем опасен Интернет для детей и как самостоятельно настроить компьютер ребенка.

ЭЛЕКС
ДОМАШНЯЯ ЭЛЕКТРОНИКА

АВТОНОМНАЯ НЕКОММЕРЧЕСКАЯ ОРГАНИЗАЦИЯ ЦЕНТР ЗАЩИТЫ ДЕТЕЙ ОТ ИНТЕРНЕТ-УГРОЗ

# Самостоятельная настройка компьютера ребенка.

## 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.

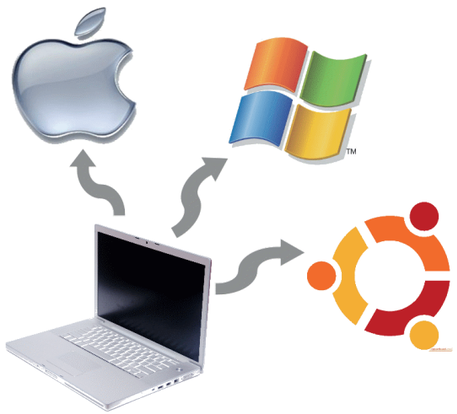
- Вы лишены техподдержки, не во всех «пиратках» возможно получать обновления безопасности.

- 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 «продвинутые» решения 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.