

Уважаемые родители!

Минимальные методы информационной безопасности для родителей

В современном информационном пространстве существует множество угроз для человека. Хищение личной информации, киберпреступность, пропаганда опасных сообществ (религиозные, асоциальные, террористические и даже криминальные). Пока у ребенка не сформировано устойчивая система ценностей, социальная позиция, мировоззрение, он легко может попасть под влияние подобных негативных факторов. Ниже приведены набор минимальных действий со стороны родителей, позволяющие на ранней стадии выявить и, по возможности, устранить информационную угрозу.

1. Включить функцию «РОДИТЕЛЬСКИЙ КОНТРОЛЬ» в браузере
2. Родителям и детям нужно составить соглашение о правилах пользования Интернетом, где будут оговорены важные моменты, которые направлены на физическую и моральную безопасность ребенка
3. Ни под каким предлогом не соглашаться на установку компьютера в комнате ребенка – он должен стоять в общей, часто посещаемой, комнате. Но не забывайте, что ребенок может выходить в сеть и по мобильному телефону
4. **Недопустимо выкладывать в сеть конфиденциальную информацию** (время возвращения из школы, место прогулок, компрометирующие фотографии) и личные данные (Ф.И.О., город, школа, адрес, возраст). Можете поучаствовать в выборе псевдонима, который не будет содержать никакой информации о ребенке
5. Предупредить ребенка не принимать приглашение собеседника на общение в приватной комнате или, что еще опаснее, соглашаться на встречу в реальной жизни и сразу сообщить об этом родителям. **Дети легко попадают под влияние** морально более сильного взрослого. Поэтому, если что-то вызовет ощущение дискомфорта, нужно сразу покинуть чат. Было бы хорошо, если бы ребенок свободно обсуждал это с родителями и не стеснялся обратиться за помощью в сомнительной ситуации
6. Оговорите с ребенком, сколько времени он может проводить в Интернете
7. Перед тем, как зарегистрироваться в чате, форме или блоге, нужно чтобы ребенок внимательно прочитал соглашение о конфиденциальности личных данных и правилах поведения чата (если какие-то пункты не ясны-проконсультироваться с родителями)
8. Для маленьких детей установите детскую поисковую систему
9. Периодически проверяйте историю посещения в браузере (не разрешайте отключать сохранение истории)

10. Ограничьте возможности по установке и настройке программного обеспечения ребенком.

Для этого воспользуйтесь правами администратора и функциями операционной системы

11. Установите лицензионное защитное программное обеспечение (антивирусную программу, фаервол, сканер шпионского ПО и т.д.)

12. Если Вы работаете через мобильного провайдера, то ознакомьтесь с сервисами безопасности, предоставляемой данной организацией (большинство провайдеров предоставляют расширенные возможности родительского контроля)

13. Для повышения общего уровня безопасности персонального компьютера установите более защищенную операционную систему (Linux Ubuntu, Linux Mint и т.д.)

14. Ознакомьтесь с материалами по теме «как защитить детей от опасностей сети ИНТЕРНЕТ?» на специализированных сайтах.

15.Повышайте свой уровень владения компьютером.