ВІДДІЛ ОСВІТИ ДЗЕРЖИНСЬКОЇ МІСЬКОЇ РАДИ

ОРІЄНТИР

МІСЬКИЙ МЕТОДИЧНИЙ КАБІНЕТ

Інформаційно-методичний вісник

№ 5 (17)
ГРУДЕНЬ 2015

БЕЗПЕЧНИЙ СЕРФІНГ ІНТЕРНЕТОМ

Світ змінюється з неймовірною швидкістю, – і розвиток комунікаційних технологій цьому сприяє. З кожним роком збільшується кількість проникнення Інтернету в наше життя.

Важливість питання безпечного Інтернету зумовлена тим, що в наш час сучасна молодь вільно володіє можливостями Інтернету та мобільних телефонів. Мережа стає більш демократичною, відкритою для великої кількості думок та форматів публікацій.

Розвиток інформаційно-комунікаційних технологій розвивається дуже бурхливо, і відповідно до цього, має відбуватись розвиток культури їх використання.

Молоде покоління - діти та підлітки - не усвідомлюють, що може чекати на них у віртуальному просторі. Значимість проблеми безпечного Інтернету потребує постійної уваги з боку школи, батьків. Одним із засобів вирішення цієї проблеми може стати просвіта громадськості та учасників освітнього процесу.

Інтернет не має національних кордонів. Тому другий вівторок лютого оголошено Міжнародним Днем безпечного Інтернету. Щорічна кампанія в Україні проходить у підтримку Європейського Дня безпечного Інтернету та покликана привернути увагу суспільства до цієї проблеми, розказати батькам про ті ризики, на які можуть натрапити діти та підлітки в Інтернеті, та як захистити себе від цих ризиків.

Ці рекомендації – практична інформація для учителів-предметників і класних керівників щодо організації позаурочної діяльності в частині використання мережі Інтернет, яка допоможе попередити загрози і зробити роботу дітей в Інтернеті корисною.

Скрипниченко Н.А.,
завідувач ММК

Думки в учительській

Інтернет - це ще одна сторіночка у розвитку людства, яку ми з часом перегорнемо як і всі інші.

Сурган В.С

Інтернет - це всього лише інструмент. Все залежить від того, хто і в яких цілях його використовує.

В Інтернеті можна знайти все, чого ти не шукаєш.

Без нього вже ніяк не можна,
Він - норма. а не дивина.
Як зрозуміти друг він нам чи ворог?
І відповідь лиш є одна;
Він - помічник,
знавець,
Порадник,
інформаційне джерело,
Але потрібно пам'ятати:
де є добро там є і зло.
І вибір все таки за вами,
Що оберемо - те і буде.

ПОСІБНИКИ, ЯКІ МІНІСТЕРСТВО ПРОПОНУЄ ВИКОРИСТОВУВАТИ БАТЬКАМ І ПЕДАГОГАМ ДЛЯ НАВЧАННЯ ДІТЕЙ БЕЗПЕЧНОМУ КОРИСТУВАННЮ ІНТЕРНЕТОМ

Діти в Інтернеті: як навчити безпеці у віртуальному світі: посібник для батьків / І. Литовченко, С. Максименко, С Болтівець [та ін.]. – К.: ТОВ "Видавничий будинок «Аванпост-Прим»", 2010. – 48 с. (http://online-bezpeka.kyivstar.ua).

- ✓ Виховання культури користувача Інтернету. Безпека у всесвітній мережі: навчально-методичний посібник / А. Кочарян, Н. Гущина. – К., 2011. – 100 с.
- ✓ (http://old.mon.gov.ua/images/newstmp/2011/18_02/3/4press.pdf).
- ✓ Безпечне користування сучасними інформаційно-комунікативними технологіями / О. Удалова, О. Швед, О. Кузнєцова [та ін.]. – К.: Україна, 2010. – 72 с.
- ✓ Пам'ятка для батьків "Діти. Інтернет. Мобільний звязок", розроблена Національною експертною комісією України з питань захисту суспільної моралі (http://www.moral.gov.ua/news/311/).
- ✓ Перелік рекомендованих для дітей онлайн-ресурсів, затверджений на засіданні Національної експертної комісії України з питань захисту суспільної моралі (рішення N 2 від 20.04.2010) (Додаток 9).

Сайт «On-ляндія» (http://www.onlandia.org.ua/) — це один з етапів реалізації Програми «Безпека дітей в Інтернеті», яку реалізують партнери Програми — Коаліція за безпеку дітей в Інтернеті. Цей сайт містить матеріали для дітей, батьків і вчителів (інтерактивні сценарії, короткі тести, готові плани уроків), завдяки яким діти зможуть освоїти **основи безпечної роботи в Інтернеті**.

Перелік рекомендованих для дітей онлайн-ресурсів, затверджений Національною експертною комісією України з питань захисту суспільної моралі (Додаток)

ОРГАНІЗАЦІЯ БЕЗПЕЧНОГО ВИКОРИСТАННЯ ІНТЕРНЕТУ УЧАСНИКАМИ ОСВІТНЬОГО ПРОЦЕСУ

Для цього:

1. Встановіть на всі домашні і шкільні комп'ютери спеціальні захисні програми, поштові фільтри та антивірусні системи для запобігання зараження програмного забезпечення і втрати даних. Такі програми спостерігають за інтернет-активністю і можуть запобігти як прямим атакам зловмисників, так і атакам, які використовують шкідливі програми (Додатки).

2. Використовуйте тільки ліцензійні програми і дані, отримані з надійних джерел. Найчастіше бувають заражені вірусами піратські копії програм, особливо ігор. Поясніть про важливість використовувати тільки перевірені інформаційні ресурси.

3. Періодично намагайтеся повністю перевіряти свої робочі комп'ютери. Для наочності в класі зробіть спеціальний стенд з Пам'яткою щодо безпечної поведінки в Інтернеті і періодично оновлюйте матеріали по даній темі. Продумайте поновлювану частину стенду. Це можуть бути новини з ігрових і розважальних сайтів для молодших класів і новинки світу програм, геймерські новини, кумедні випадки соціальних мереж, інтернет-гумор і курйози – для старших школярів. Полегшений контент буде врівноважувати дидактичний характер Пам'ятки, але і буде змушувати постійно звертатися до неї, як до інформації, що сусідить із забавним і постійно обновлюваним блоком.

Безпечний Інтернет

МЕТОДИЧНІ РЕКОМЕНДАЦІЇ

✓ **для вчителів початкової школи**

Діти в цьому віці приділяють Інтернету не менше уваги, чим більш дорослі. У дітей цього віку зазвичай відкрита натура і позитивний погляд на світ. Діти цього віку повинні виходити в Інтернет спочатку тільки під наглядом вчителів або батьків на сайти, які відповідають віком і культурного розвитку дитини.

Основні правила безпечної поведінки в Інтернеті для учнів початкових класів

- Завжди запитуйте батьків про незнайомі речі в Інтернеті: вони розкажуть, що безпечно робити, а що – ні.
- Перш ніж почати товаришувати з кимось в Інтернеті, запитайте у батьків, як безпечно спілкуватися.
- Ніколи не розповідайте про себе незнайомим людям, де ви живете, навчаєтесь, номер телефону тощо.
- Не відправляйте фотографії людям, яких ви не знаєте. Не потрібно, щоб незнайомі люди бачили фотографії вас, ваших друзів або членів вашої родини.
- Не зустрічайтесь без батьків з людьми, з якими познайомились в Інтернеті. В Інтернеті багато людей розповідають про себе неправду.
- Спілкуючись в Інтернеті, будьте дружелюбні з іншими. Не пишіть грубих слів. Читати грубощі так само неприємно, як і чути. Ви можете ненавмисно образити людину.
- Якщо в Інтернеті вас хтось засмутив чи образив, обов’язково розкажіть про це батькам.

✓ **для вчителів середньої школи.**

Саме з переходом у вікову категорію «підліток» проблеми, пов’язані з Інтернетом, стають дійсно гострими і глобальними. Що ж підстерігає дітей підліткового віку з екрана монітора, які проводять біля комп'ютера досить багато часу:

- ✓ Порнографія. Небезпечна надлишковою інформацією і грубим, часто збоченим, натуралізмом. Заважає розвитку природних емоційних прихильностей.
- ✓ Депресивні молодіжні течії. Дитина може повірити, що шрами – краща прикраса, а суїцид – всього лише спосіб позбавлення від проблем.
- ✓ Наркотики. Інтернет рясніє новинами про «користь» вживання марихуани, рецептами і порадами виготовлення «зілля».
- ✓ Сайти знайомств, соціальні мережі, блоги і чати. Віртуальне спілкування руйнує здатність до спілкування реального, модифікує комунікативні навички, які ми природно здобуваємо в процесі соціалізації в живому людському спілкуванні.
- ✓ Секти. Віртуальний співрозмовник не схопить за руку, але йому цілком по силам «проникнути в думки» і вплинути на погляди на світ.
- ✓ Екстремізм, націоналізм, фашизм. Всі широкі можливості Інтернету використовуються представниками екстремістських течій для того, щоб заманити в свої ряди новачків.

Всі вищевикладені технічні і методологічні рекомендації для школярів молодшого шкільного віку залишаються в силі і для підлітків. Але це не панацея від усіх бід, бо часом школярі є набагато більш просунутими користувачами, здатними обійти будь-які обмеження з серфінгу в Інтернеті. Тому фільтри – це лише тимчасова ефективна міра. У цій роботі важливіше за все узгоджена робота школи і батьків і посилення виховної загально гуманітарної роботи.

Безпечний Інтернет

Можна запропонувати учням скласти свої принципи спілкування у Інтернеті. Розгляньте разом з учнями детальніше неформальний кодекс поведінки в мережі Інтернет, що регулює спілкування користувачів один з одним і так званий нетикет (netiquette – від злиття англ. слів net – мережа і etiquette – етикет) або мережевий етикет. Мережевий етикет – це декілька базових правил поведінки в мережі, однак ці правила час від часу піддаються змінам: щось застаріває і втрачає свою актуальність у зв'язку з розвитком технологій Інтернет, а щось додається нове.

Мережевий етикет регулює:

- ✓ правила обміну повідомленнями по електронній пошті;
- ✓ стилістику мережевої комунікації при колективних обговореннях;
- ✓ загальні правила написання публікованих текстів у мережі і пр.

При листуванні по електронній пошті кожен користувач повинен пам'ятати про деякі правила:

- ✓ вітайте співрозмовника на початку листа і прощайтеся в кінці;
- ✓ по електронній пошті можна звертатися до незнайомих людей, але за умови, що адресу було опубліковано його власником;
- ✓ пишіть коротко, грамотно і акуратно;
- ✓ при відповіді на повідомлення треба цитувати його найбільш істотні місця;
- ✓ зручно, коли листи користувача закінчуються коротким «підписом», що автоматично додається до кожного повідомлення, надсилання користувачем, однак цей підпис не має бути довше чотирьох-п'яти рядків; дуже важливо вказати в підписі своє ім'я по батькові повністю, щоб було зручно одержувачу звернутися до Вас;
- ✓ у листуванні особистого характеру можна дотримуватися розмовного стилю;
- ✓ не слід переправляти чиєсь особисте повідомлення іншим людям або в телеконференцію без попередньої згоди його автора;
- ✓ якщо ви зайняті і не можете швидко відповісти на повідомлення, відправте пару рядків з підтвердженням отримання і обіцянкою відповісти при першій можливості;
- ✓ якщо повідомлення надійшло від незнайомої особи, слід зрозуміти, обґрунтовано воно чи ні. У першому випадку – відповісти протягом трьох днів. У другому – не відповідати;
- ✓ текст листа потрібно структурувати за змістом, абзаци відділяти порожнім рядком;
- ✓ якщо ви відправляєте заархівований файл, поцікавтеся заздалегідь, чи зможе одержувач листа його розпакувати;
- ✓ рядок тексту повинен обмежуватися 60-70 символами, праворуч без вирівнювання;
- ✓ небажано надсилати листи великого змісту, оскільки користувач, який працює з безкоштовною поштовою скринькою, може таке послання не прочитати через обмеження обсягу вхідної кореспонденції;
- ✓ якщо до листа прикріплений файл, то в тексті листа обов'язково повинно було зазначено, що він містить і навіщо.

Будь відповідальним – і в реальному житті, і в Мережі. Просте правило: якщо ти не будеш робити чогось в реальному житті, не варто це робити онлайні. Коли ти поводишся нечемно в Інтернеті співрозмовнику, ти провокуєш його на таку ж поведінку. Спробуй залишатися ввічливим або просто не реагувати.

Все, що ти розміщуєш в Інтернеті, назавжди залишиться з тобою – як татуювання. Тільки ти не зможеш цю інформацію видалити або контролювати її використання. Адже ти не хочеш виправдовуватися за свої фотографії перед майбутнім роботодавцем?

Безпечний Інтернет

Основні правила безпечної поведінки в Інтернеті для учнів середніх класів

- При реєстрації на сайтах намагайтесь не вказувати особисту інформацію, оскільки вона може бути доступною незнайомим людям. Також не рекомендується розміщати свої фото, даючи тим самим уявлення, як ви виглядаєте, абсолютно незнайомим людям.
- Якщо ви публікуєте фото чи відео в Інтернеті, їх може подивитися кожен. Зважайте на це.
- Використовуйте веб-камеру лише при спілкуванні з друзями, родичами. Прослідкуйте, щоб сторонні люди не мали змоги бачити вашу розмову, оскільки вона може бути записана.
- Небажані листи від незнайомих людей називаються «спам». Якщо ви отримали такого листа, не відповідайте на нього. В разі, коли ви дасте на нього відповідь, відправник буде знати, що ви користуєтесь цією поштовою скринькою і буде продовжувати надсилати вам спам.
- Якщо вам прийшов лист з невідомої адреси, краще не відкривайте його. Такі листи можуть містити віруси.
- Якщо вам надходять листи з неприємним, ображаючим змістом, якщо хтось поводить себе по відношенню до вас негідним чином, повідомте про це дорослих.
- Пам’ятайте, що віртуальні знайомі можуть бути не тими, за кого себе видають.
- Якщо поруч з вами немає когось з дорослих, яким ви довіряєте і які можуть вас захистити, не зустрічайтесь в реальному житті з людьми, з якими ви познайомились в Інтернеті. Якщо ваш віртуальний друг справді той, за кого себе видає, він спокійно зреагує на вашу турботу про власну безпеку.
- Ніколи не пізно розповісти дорослим, якщо вас хтось образив.

Інформаційні матеріали, які можуть бути використані при проведенні просвітницьких заходів з батьками учнів щодо безпечного перебування їхніх дітей у мережі Інтернет

Спеціальні класні години необхідно присвятити бесідам з батьками про правила забезпечення безпеки дітей у роботі з Інтернетом вдома. І хоча багато батьків вважають себе просунутими користувачами і впевнені в тому, що з їх дітьми нічого поганого в мережі відбутися не може, це не так. Навіть такі батьки повинні розуміти, що з’являються самі по собі рекламні банери порно-сайтів, нав'язливі торгові гасла – це небезпечні пастки для їх непідготовлених поки до соціально-агресивного світу Інтернету дітей.

По-перше, потрібно розповісти, як обмежити пошук в мережі Інтернет, зробити його безпечним (найпростіший - обмежити пошук в браузері). Можна запропонувати посібник для батьків «Діти в Інтернеті», розроблений компанією "Київстар"- національним лідером телекомунікацій разом з інститутом психології ім. Г.С. Костюка Національної академії педагогічних наук України.

РЕКОМЕНДАЦІЇ, ЯКІ СТАНУТЬ У НАГОДІ ТУРБОТЛИВИМ БАТЬКАМ, ЩО ПРАГНУТЬ ЗРОБИТИ РОБОТУ ДІТЕЙ В ІНТЕРНЕТІ КОРИСНОЮ.

Правило 1.

Уважно ставтесь до дій вашої дитини у мережі Інтернет:

- ✓ не відправляйте дитину у «вільне плавання» по Інтернету, намагайтесь активно брати участь у взаємодії дитини з мережею, особливо на етапі її освоєння;
- ✓ спілкуйтесь з дитиною про те, що нового вона дізнається для себе за допомогою Інтернету і як вчасно попередити загрози.
- ✓ не забувайте про те, що заборонені ресурси можуть завантажуватися автоматично під час відвідування сайтів з контентом, який не містить небезпеки для дітей. Тож не варто одразу сварити дитину за відвідування сайтів із небажаним контентом — вона могла бути абсолютно до цього не причетною.

Правило 2.

Інформуйте дитину про можливості і небезпеки, які містить у собі мережа:

- ✓ поясніть дитині, що в Інтернеті, як і в житті, зустрічаються «гарні» і «погані» люди; переконайте, що в разі зіткнення дитини з негативом чи насильством з боку іншого користувача, вона має повідомити про це близьких людей;
- ✓ навчіть дитину шукати потрібну інформацію і перевіряти її, в тому числі, з вашою допомогою;
- ✓ навчіть дитину уважно ставитися до скачування платної інформації і отримання платних послуг з Інтернету, особливо через відправлення смс-повідомлень;
- ✓ складіть перелік корисних, цікавих, безпечних ресурсів, якими може користуватися ваша дитина, і порадьте їй їх використовувати.

Правило 3.

Оберіть зручну форму контролю перебування вашої дитини в мережі:

- ✓ встановіть на вашому комп'ютері необхідне програмове забезпечення – програми батьківського контролю, антивіруси;
- ✓ якщо ваша дитина навчається у початкових класах, обмежте час її перебування в Інтернеті; якщо в середніх чи старших – домовтесь про режим користування Інтернетом;
- ✓ якщо комп'ютер використовують усі члени родини, встановіть його в місці, доступному для всіх, а не в кімнаті дитини;
- ✓ створіть різні облікові записи на вашому комп'ютері для дорослих і дитини; це допоможе не тільки убезпечити дитину, але й зберегти ваші дані;
- ✓ регулярно відстежуйте ресурси (перевіряйте історію браузера); прості налаштування комп'ютера дозволять вам бути в курсі того, яку інформацію переглядала ваша дитина. , щоб розуміти, якими сайтами та сервісами користається дитина.

Правило 4.

Регулярно підвищуйте рівень власної комп'ютерної грамотності, щоб забезпечити безпеку дитини:

- ✓ використовуйте зручні можливості підвищення рівня комп'ютерної та Інтернет-грамотності: відвідування курсів, читання спеціальної літератури, консультації з експертами;
- ✓ знайомте членів вашої родини з базовими принципами безпечної роботи на комп'ютері і в Інтернеті.

Безпечний Інтернет

МАТЕРІАЛИ ДЛЯ ПРОВЕДЕННЯ КЛАСНИХ ГОДИН

Мета: навчання інформаційній безпеці в Інтернеті, розвиток самоконтролю учнів і формування уважного та відповідального ставлення до інформаційних ресурсів, формування культури комунікацій в мережі.

Питання для розгляду:

- перелік ризиків, які можуть спіткати учня в Інтернеті;
- правила розміщення особистої інформації в мережі;
- захист особистих даних;
- способи безпечного спілкування в режимі онлайн;
- доцільна організація робочого часу і часу на дозвілля – ефективний засіб профілактики Інтернет-залежності;
- правила безпеки в мережі Інтернет;
- віртуальні друзі чи шахраї та злодії?;
- захист від спаму та вірусів;
- критичний підхід до інформації.

Питання для обговорення:

- Чи траплялись з вами неприємні випадки у школі, вдома, пов'язані з Інтернетом? (наприклад, хтось образив, обдурив)
- Як убезпечити себе від неприємних ситуацій в Інтернеті?
- Чи можете ви створити загрозу для когось з користувачів? У якому випадку?
- Чи погоджуєтесь ви з думкою, що Інтернет – це вільний простір, у якому можна робити все, що забажаєш?
- Як ви вважаєте, чи шкодить Інтернет вашому фізичному здоров'ю? Чому?
- Як ви вважаєте, чи шкодить Інтернет вашій моралі? Чому?
- Як ви вважаєте, чи шкодить Інтернет вашому психічному здоров'ю? Чому?
- Як ви вважаєте, чи шкодить Інтернет вашому культурному рівню? Чому?
- Які ви знаєте правила користування ресурсами Інтернету?

Завдання для учнів:

- знайти сайти, присвячені безпеці дітей і підлітків в Інтернеті, скласти їх анотований каталог;
- сформулювати у підгрупах по 5 найважливіших правил безпечної поведінки в мережі Інтернет, обґрунтувати їх важливість, зробити посилання на сайти, де це правило зустрічається;
- виробити спільні правила безпечної поведінки в Інтернеті, оформити їх у вигляді плакату, інформаційного бюлетеня тощо, розмістити на сайті школи;
- знайти в Інтернеті приклади порушень правил безпеки та етикету спілкування; визначити, яке саме правило порушено, запропонувати можливі шляхи виправлення ситуації з порушеннями правил безпеки та етикету спілкування в мережі;
- підготувати інформаційні матеріали з безпеки в Інтернеті і представити їх учням молодших класів у цікавій формі (казка, гра, вікторина тощо).

Можуть бути проведені наступні заходи з безпеки дітей в Інтернеті:

- виховні години, бесіди з теми «Безпечний Інтернет»;
- конкурс мультимедійних презентацій з теми «Безпека дітей в Інтернеті»;
- конкурс стіннівок та малюнків «Безпека дітей в Інтернеті»;
- випуск шкільної газети, стаття "Інтернет - помічник чи пастка для молоді";
- ***обговорення на сайті ЗНЗ або у блогах «Як ми провели День Безпеки Інтернету»;***
- ігрові заняття "Безпека в Інтернеті" для учнів початкової школи;
- виставка фотографій, картинок, зображень «Я – за безпечний Інтернет»;
- тренінг для учнів "Безпечний Інтернет";
- конференція або форум "Діти в Інтернеті: реальні небезпеки віртуального світу";
- опитування серед учнів, батьків, вчителів, присвячене оцінці ризиків та безпеки в Інтернеті;
- виступи на батьківських зборах "Безпека Ваших дітей в Ваших руках".

ФІЛЬТРАЦІЯ КОНТЕНТУСЕРВІСІВ ІНТЕРНЕТ В НАВЧАЛЬНИХ ЗАКЛАДАХ

Для забезпечення посилення контролю використання мережі Інтернет в освітніх цілях та обмеження доступу учнів ЗНЗ до забороненого і небажаного контенту Інтернет- ресурсів повинна бути проведена низка організаційних та технічних заходів.

По-перше, у кожному освітньому закладі, де існує вихід до мережі Інтернет, у вільному доступі знаходяться законодавчі та інші нормативні акти **(**Типові правила використання мережі Інтернет в загальноосвітньому закладі, які регулюють умови та порядок використання мережі Інтернет через ресурси загальноосвітньої установи учням), які мають статус локального нормативного акту Освітньої установи, режиму роботи комп'ютерного класу.

До роботи в мережі Інтернет допускаються особи, що пройшли інструктаж і зобов'язалися дотримуватися правил роботи. Тільки після ознайомлення з даними документами починаючий користувач може працювати в мережі Інтернет у навчальному закладі.

Викладачами навчальних закладів проводяться виховні години, лекції щодо грамотного та безпечного використання Інтернет-ресурсів, проводиться знайомство з сайтом «Онляндія – безпечний Інтернет». На батьківських зборах можна запропонувати поради щодо налаштування батьківського контролю вдома.

По-друге, забезпечити впровадження програмно-технічних засобів, що обмежують доступ до мережі ресурсів Інтернет.

Крім того, у вільному доступі повинні знаходитися правила Інтернет-безпеки та Інтернет-етики для учнів, пам'ятка по використанню ресурсів мережі Інтернет учнями навчального закладу під час навчальних занять.

ЗАКЛЮЧЕННЯ

Зупинити прогрес неможливо, і його не треба боятися. Сучасному учителю треба приймати інформаційно - комунікаційний потік з гідністю і не тільки озброївшись знаннями, вміннями і навичками, але і компетентністю, ініціативою, творчим настроєм. Вчителю треба відчути свою величезну роль у сучасному світі, в тому числі і віртуальному, і підлаштовувати віртуальний світ під себе, а не підлаштовуватися під нього. Ми, люди, створили цей цифровий світ, значить і ми відповідаємо за все, що там відбувається. Значить, ми можемо керувати ним, тому що все в наших руках.

Безпечний Інтернет

ІНСТРУКЦІЯ ДЛЯ ВЧИТЕЛЯ ПРО ПОРЯДОК ДІЙ ПІД ЧАС ЗДІЙСНЕННЯ КОНТРОЛЮ ЗА ВИКОРИСТАННЯМ УЧНЯМИ МЕРЕЖІ ІНТЕРНЕТ

1. Ця інструкція регламентує порядок дій вчителя в разі виявлення:
   - ✓ звернення слухачів до контенту, що не стосується навчального процесу;
   - ✓ відмови при зверненні до контенту, що має відношення до навчального процесу, викликаної технічними причинами;
   - ✓ контроль використання учнями мережі Інтернет здійснюють, вчителем, що проводить заняття.

2. Вчитель:
   - ✓ визначає час і місце роботи учнів з врахуванням використання в навчальному процесі відповідних технічних можливостей, а також тривалість сеансу роботи одного учня;
   - ✓ на початку заняття, коли комп'ютери ще не ввімкнені, інструктує учнів про техніку безпеки і правила користування комп'ютером та від чого необхідно утриматися під час дослідження Інтернету;
   - ✓ спостерігає за використанням школярами комп'ютерів і мережі Інтернет (не дозволяє марно блукати в Інтернеті – оптимально вибрати кілька сайтів, що становлять інтерес і зосередити на них увагу учнів);
   - ✓ забороняє подальшу роботу учня в мережі Інтернет на занятті в разі порушення ним порядку використання мережі Інтернет і вимог до учнів під час роботи в мережі Інтернет;
   - ✓ вживає необхідних заходів з недопущення звернень до ресурсів, що не стосуються навчального процесу.

3. В разі виявлення ресурсу, котрий, на думку вчителя, містить інформацію, заборонену для розповсюдження у відповідності з законодавством України, чи іншого потенційно небезпечного для слухачів контенту, він повідомляє про це адміністраторам ЗНЗ.

ЖУРНАЛ РЕЄСТРАЦІЇ КОРИСТУВАЧІВ МЕРЕЖІ ІНТЕРНЕТ

№	П.І.Б.	Дата роботи в мережі	Адреса сайту або ресурсу	Час початку роботи	Час закінчення роботи	Розпис	Розпис відповідальн. за «точку доступу»
1							
2							
3							
4							

ЖУРНАЛ ВСТУПНОГО ІНСТРУКТАЖУ КОРИСТУВАЧІВ МЕРЕЖІ ІНТЕРНЕТ З ПРАВОВИМИ ТА НОРМПТИВНИМИ

№	П.І.Б.	Клас	Дата проведення інструктажу	Ознайомлений / не ознайомлений	Розпис інструктували	Розпис інструктує
1						
2						
3						
4						

Безпечний Інтернет

ПАМ'ЯТКА ПО ВИКОРИСТАННЮ РЕСУРСІВ МЕРЕЖІ ІНТЕРНЕТ УЧНЯМИ НАВЧАЛЬНОГО ЗАКЛАДУ ПІД ЧАС НАВЧАЛЬНИХ ЗАНЯТЬ

- Адміністратором локальної мережі в комп'ютерному класі є вчитель.
- При вході в кабінет, необхідно звернутися до вчителя за дозволом на роботу на робочій станції. Для доступу до Інтернет та використання електронної пошти установлений програмний продукт "InternetExplorer","OutlookExpress".
- Відправлення електронної пошти з приєднаною до листа інформацією, запис інформації на дискети та CD- диски здійснюється при нагляді вчителя.
- На початку роботи учень **повинен ознайомитись з правилами роботи в мережі Інтернет та** зареєструватися в системі, тобто ввести своє реєстраційне ім'я та пароль. Після закінчення роботи необхідно завершити свій сеанс роботи, викликавши в меню "Пуск" команду "Завершение сеанса<ім'я>" або в меню "Пуск" команду "Завершение работы" и "Войти в систему под другим именем".
- За одним робочим місцем не повинно знаходитися більше одного користувача.
- **Забороняється** працювати під чужим реєстраційним ім'ям, повідомляти будь-кому свій пароль, одночасно входити в систему більш ніж з однієї робочої станції.
- Кожен учень за наявності технічної можливості може мати **персональний каталог**,призначений для зберігання особистих файлів загальним обсягом не більше 5 Мб. Аналогічно може бути надана можливість роботи з поштовою скринькою.
- В разі виникнення проблем необхідно звернутися до вчителя інформатики.
- **Дозволяється** використовувати обладнання класів лише для роботи з інформаційними ресурсами та електронною поштою і лише в освітніх цілях або для здійснення наукових досліджень, виконання проектів. Будь-яке використання обладнання в комерційних цілях заборонене.
- **Заборонена** передача зовнішнім користувачам інформації, що становить комерційну чи державну таємницю, розповсюджувати інформацію, що порочить честь та гідність громадян. Правові відносини регулюються Законами України "Про інформацію", "Про державну таємницю", "Про авторське право і суміжні права", статтями Конституції України, статтями Цивільного та Кримінального кодексів про злочини у сфері комп'ютерної інформації.
- **Забороняється** працювати з об'ємними ресурсами (відео, аудіо, чат, ігри) без погодження з вчителем.
- **Забороняється** доступ до сайтів, що містять інформацію сумнівного змісту та що суперечить загальноприйнятій етиці.
- Користувачу **заборонено** вносити будь-які зміни в програмне забезпечення, встановлене як на робочій станції, так і на серверах, а також здійснювати запис на жорсткий диск робочої станції.
- Забороняється перезавантажувати комп'ютер без погодження з вчителем інформатики.
- Користувач повинен зберігати обладнання у повній цілості.
- В разі заподіяння будь-яких збитків (псування майна, виведення обладнання з робочого стану) **учень** несе **матеріальну відповідальність.**
- В разі порушення правил роботи учень позбавляється доступу до мережі.
- За адміністративне порушення, що не тягне за собою псування майна, виведення обладнання з робочого стану і що не суперечить прийнятим правилам роботи користувач отримує перше попередження.
- В разі повторного адміністративного порушення учень**позбавляється доступу до Інтернет** без права відновлення.

Безпечний Інтернет

ПРАВИЛА КОРИСТУВАННЯ МЕРЕЖЕЮ ІНТЕРНЕТ

- Доступ до Інтернет здійснюється в контексті культурних, інформаційних, освітніх потреб користувачів.
- Користування Інтернетом безкоштовне.
- Доступ до Інтернету для користувачів надається за попереднім запитом за розкладом.
- Учень зобов'язаний:

  - ✓ повідомити про вид потрібних послуг і тематику інформаційного запиту;
  - ✓ дбайливо ставитися до комп'ютерного обладнання і програмного забезпечення;
  - ✓ при необхідності копіювання інформації повідомити вчителя;
  - ✓ повідомити вчителя про неполадки і порушення, що виникли;
  - ✓ компенсувати нанесені матеріальні збитки у випадку виникнення таких.

- **Забороняється:**

  - ✓ перегляд та розповсюдження в мережі Інтернет матеріалів, заборонених чинним законодавством України;
  - ✓ використовувати Інтернет для комерційних (розміщення реклами і т.п.), протизаконних (порушення авторських прав і ін.) і неетичних (перегляд сайтів порнографічного змісту та ін.) цілей, а також для нанесення шкоди чи збитків іншим особам чи організаціям;
  - ✓ інсталювати будь-яке програмне забезпечення з Інтернет або з власних носіїв інформації на комп'ютери в навчальному закладі;
  - ✓ направляти заявки, заповнювати електронні анкети, пов'язані з відправленням будь-якого роду кореспонденції по електронних каналах;
  - ✓ завантажувати з Інтернет у архівні файли, які саморозпаковуються;
  - ✓ копіювати з Інтернету файли з розширенням *.com, *.exe без дозволу;
  - ✓ підключатися до мережевих комп'ютерних ігор;
  - ✓ вносити зміни в настроювання комп'ютера і програмного забезпечення;
  - ✓ виключати або перезавантажувати комп'ютер;
  - ✓ порушувати навчальну атмосферу закладу (голосно розмовляти, користуватись мобільним телефоном, заважати роботі іншим учням, користуватися, сайтами знайомств);
  - ✓ неправомірно "скачувати" і використовувати ліцензії на програмне забезпечення.

<u>У разі порушення правил користування вчитель має право припинити роботу в Інтернет мережі.</u>

Безпечний Інтернет

ПРАВИЛА ІНТЕРНЕТ – БЕЗПЕКИ ТА ІНТЕРНЕТ - ЕТИКИ ДЛЯ ДІТЕЙ І ПІДЛІТКІВ

- Ніколи не давайте особистої інформації про себе (прізвище, номер телефону, адресу, номер школи) без дозволу батьків.
- Якщо ви віднайшли в мережі щось, що бентежить вас, не намагайтеся розібратися в цьому самостійно. Зверніться до батьків або вчителів вони знають, що треба робити.
- Зустрічі в реальному житті зі знайомими по Інтернет-спілкуванню не є дуже гарною ідеєю, оскільки люди можуть бути дуже різними в електронному спілкуванні і під час реальної зустрічі. Якщо ж ви все_таки хочете зустрітися з ними, повідомте про це батьків, і нехай вони підуть на першу зустріч разом із вами.
- Не відкривайте листи електронної пошти, файли або web-сторінки, отримані від людей, яких ви реально не знаєте або яким не довіряєте.
- Нікому не давайте свій пароль, за винятком дорослих вашої родини.
- Завжди дотримуйтеся сімейних правил Інтернет-безпеки: вони розроблені для того, щоб ви почувалися комфортно й безпечно в мережі.
- Ніколи не робіть того, що може призвести до грошових витрат у вашій родині, окрім випадків, коли поруч із вами батьки.
- Завжди будьте ввічливими в електронному листуванні, і ваші респонденти будуть ввічливими з вами.
- В електронних листах не користуйтеся верхнім регістром, це сприймається в мережі як крик і може прикро вразити вашого співрозмовника.
- Не надсилайте в листі інформацію великого обсягу (картинки, фотографії тощо) без попередньої домовленості з вашим співрозмовником.
- Не розсилайте листи з будь_якою інформацією незнайомим людям без їхнього прохання, це сприймається як спам і, звичайно, засмучує користувачів мережі.
- Завжди поводьтеся в мережі так, як би ви хотіли, щоб поводилися з вами.

Безпечний Інтернет

ОБМЕЖЕННЯ ДОСТУПУ ДО НЕБАЖАНИХ ДЛЯ ПЕРЕГЛЯДУ РЕСУРСІВ

З технічної точки зору, інструменти для обмеження доступу до сайтів з небажаним змістом можна розділити на самостійні програми і всілякі доповнення до браузерів. З точки зору функціоналу – це додатки для системних адміністраторів і батьків, які бажають обмежити як перелік ресурсів, так і час доступу до мережі для користувачів, а також фільтри контенту для свідомих користувачів, які хочуть обмежити вплив на себе агресивного середовища інтернет.

Існує відносно простий спосіб заблокувати доступ до сайтів з підозрілим змістом: потрібно використати можливості роутера (якщо такий пристій є в локальній мережі). В багатьох моделях присутні найпростіші функції блокування певних інтернет-вузлів. В деяких забороняються конкретні URL-адреси, а інші дозволяють використовувати ключові слова. Наприклад, ввівши ключове слово "sex", ви зможете заблокувати цілий ряд ресурсів, в адресі яких присутня дана комбінація букв. Зручно і те, що в моделях з подібною функціональністю, як правило, є опція планування, яка дозволяє обмежити роботу фільтра за часом і в певні дні тижня. Даний метод захисту досить ефективний, однак є моделі роутерів, в яких механізм додавання заборонених адрес чи ключових слів реалізований невдало: одночасно можна ввести всього одну адресу або слово.

Ще один спосіб обмежити дитині доступ до небажаної інформації - використати так званий дитячий браузер, наприклад, розширення до Mozilla Firefox з трохи дивною назвою "Гогуль" (www.gogul.tv). Важливим фактором є те, що "Гогуль" - це проект орієнтований на російськомовного користувача. На відміну від альтернативних рішень, у випадку з якими потрібно самостійно вказувати ненадійні сайти і складати список дозволених, тут перелік останніх уже існує. Він включає розважальні, спортивні і освітні ресурси. Цей набір досить цікавий: це саме сайти для дітей, з яскравими сторінками і відповідним змістом. Перед початком роботи потрібно зареєструватися і створити батьківський обліковий запис. Тоді можна зайнятися створенням дитячих аккаунтів, вказавши для кожного дозволені дні і час роботи в Мережі. В результаті після запуску браузер буде пропонувати вибрати один з облікових записів. В особистому кабінеті батьки мають можливість додавати нові ресурси в каталох дозволених сайтів. Також там можна отримати доступ до статистики сторінок, які відвідує дитина і часу, який вона проводить в Інтернет. Крім того, з сайту можна скачати додаток Angry Duck. Він дозволяє за бажанням батьків блокувати запуск всіх браузерів, крім "Гогуль", обмежувати доступ до файлів і папок. Також Angry Duck дозволяє відстежувати програми, що запускаються на комп'ютері.

Крім того, у пошукових систем існує прекрасна безкоштовна послуга — налаштування безпечного або сімейного фільтра. Не полінуйтеся і знайдіть за допомогою «Запитай як» ці функції у себе в браузері.

Наприклад: Налаштування Firefox

Заходимо в Інструменти->Налаштування.., переходимо на вкладку Додатково -> Мережа і тиснемо на кнопочку Настроїти

Ще один спосіб створити бар'єр між дитиною і інтернетом - встановити на комп'ютер проксі-сервер, налаштувати браузер для роботи з ним (для локальної машини достатньо в параметрах браузера вказати адресу 127.0.0.1). Можна використати, наприклад, безкоштовну версію Tmetr (www.tmetr.ru). В такому випадку ви отримуєте можливість обмежувати швидкість трафіку, блокувати URL як в цілому так і за ключовими словами, отримувати детальні звіти про переміщення користувачів в Мережі. Однак, цей спосіб має і свої недоліки. По-перше, доведеться розбиратися в досить запутаному інтерфейсі програми. По-друге, чорні та білі списки доведеться створювати самостійно. До того ж відключити проксі-сервер значно простіше ніж спеціалізовану програму.

Безпечний Інтернет

ОБМЕЖЕННЯ ДОСТУПУ ДО НЕБАЖАНИХ ДЛЯ ПЕРЕГЛЯДУ РЕСУРСІВ

З технічної точки зору, інструменти для обмеження доступу до сайтів з небажаним змістом можна розділити на самостійні програми і всілякі доповнення до браузерів. З точки зору функціоналу – це додатки для системних адміністраторів і батьків, які бажають обмежити як перелік ресурсів, так і час доступу до мережі для користувачів, а також фільтри контенту для свідомих користувачів, які хочуть обмежити вплив на себе агресивного середовища інтернет.

ПРОГРАМИ:

Інтернет-Цензор.
Сайт: http://www.icensor.ru/

Цей додаток відфільтровує сайти, занесені до чорного списку. Спеціальна група експертів відбирає ці ресурси з усього російськомовного сектору мережі вручну. Існує також «білий» список, який постійно оновлюється і в найближчому майбутньому планується додати англомовні ресурси. Дитина не зможе внести зміни в налаштування або видалити програму з комп'ютера. Доступ до налаштувань програми здійснюється за допомогою пароля, заданого в процесі установки, а його нагадування приходить на e-mail, вказаний тоді ж.

Один дома
Сайт: http://odindoma.org/

Це програма-фільтр, що захищає дитину в мережі Інтернет від негативної інформації та "дорослих", порно-сайтів.

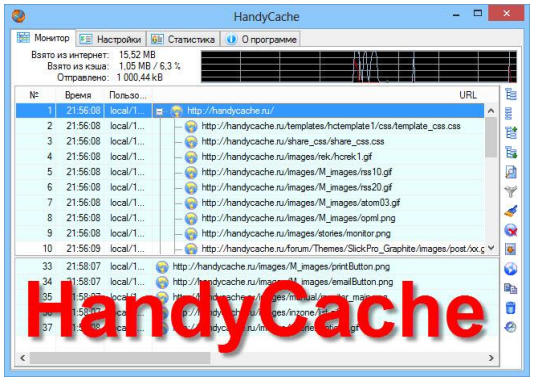
Ознайомитися з програмою можна, якщо закачати безкоштовно повну версію програми на 3 дні з офіційного сайту. Крім того, програму можна купити on-line, отримавши пін-код після оплати з допомогою смс або е-грошей. Програму можна також замовити у коробочній версії, залишивши заявку на офіційному сайті.

КіберМама

Програма для батьків, що дозволяє планувати, контролювати і обмежувати роботу дітей на домашньому комп'ютері. Перериває роботу комп'ютера після закінчення дозволеного кількості часу, або згідно з розкладом, а також блокує доступ до різних програм, в тому числі ігор. Має режими роботи «Батько» і «Дитина». Доступ до адміністрування програми захищений паролем. Програма платна, доступна тимчасова демо-версія.

Безпечний Інтернет

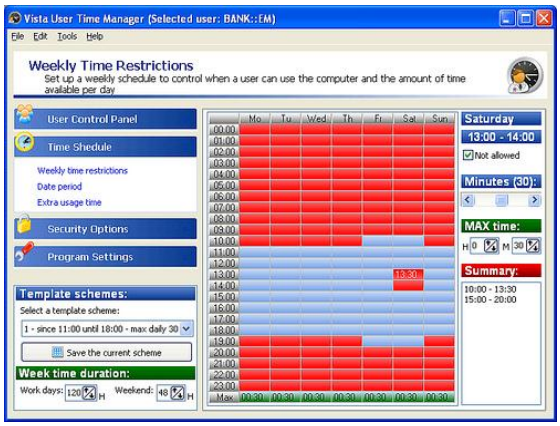
HandyCache
Сайт http://handycache.ru/



HandyCache – це безкоштовна програма, яка економить трафік, прискорює завантаження сторінок, блокує рекламу і дозволяє в автономному режимі (без підключення до Інтернет) проглянути будь-які відвідані раніше сайти.
HandyCache – це кешуючий проксі-сервер. Він скорочує трафік до 3-4 разів за рахунок кеша: одного дня завантажені сторінки (файли) записуються в кеш і при наступному запиті беруться з кеша, а не з Інтернет - за рахунок цього економляться і трафік і час завантаження.

Будь-якою зі встановлених на комп'ютері браузерів (і інші програми) можуть використовувати кеш HandyCache, а значить, немає необхідності завантажувати одні і ті ж сторінки кілька разів для перегляду в різних браузерах. Більш того, і без підключення до Інтернет можна переглядати відвідані раніше сторінки і завантажені файли. Щоб оцінити HandyCache в роботі, потрібно його завантажити, встановити і вказати HandyCache проксі-сервером в браузері. Для початку роботи цього вистачає: налаштування, встановлені за умовчанням, підходять для більшості випадків, але для тонкого налаштування варто зупинитися на декількох моментах.

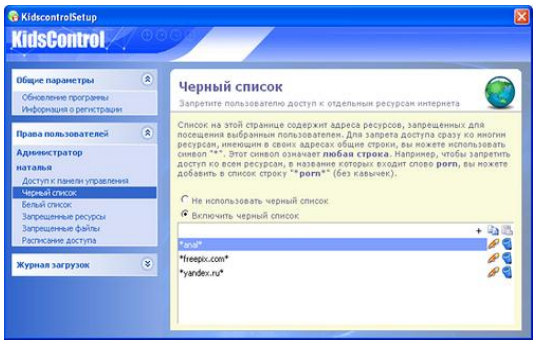
Parental Control Tool і Kids PC Time Administrator



Програма, яка дозволяє керувати, обмежувати і контролювати користувачів. Можете заблокувати використання будь-яких додатків користувачем. Батьки можуть самостійно визначати, скільки часу їх діти можуть проводити за комп’ютером або в Інтернеті. Також можна закрити доступ до сайтів з небажаним вмістом, наприклад, програма автоматично блокувати доступ до сайтів, які містять ключові слова «секс» або «порно», як на сторінці, так і в самій назві.

Безпечний Інтернет

KidsContro.



Дозволяє настроїти обмеження доступу до небажаних ресурсів по різних категоріях – сайтам, з вмістом інформації для дорослих, online-ігор і казино, форумів, вказавши галочкою на певну категорію, і встановити обмеження самостійно за допомогою чорного списку. Також тут є можливість задати контроль доступу до Інтернету по днях і годинах, тобто налаштувати розклад роботи.

Дитячий браузер: Гогуль

Гогуль побудований на тому ж принципі, що і Бруз – це теж аддон Firefox. Гогуль забезпечує контроль відвідування дитиною сайтів в інтернеті. Для контролю запуску інших браузерів можна скористатися безкоштовним доповненням – програмою Angry Duck (Зла Качка). Домашня сторінка браузера – портал gogul.tv пропонує досить цікавий набір розвиваючих і пізнавальних інтернет-ресурсів для дітей.

Плагіни та панелі:

Suricate Collaborative parental control

Плагін для Firefox. Блокує як цілі сайти, з контентом 18, так і окремі зображення з заборонених адрес. «Чорний» список формується користувачами за допомогою кнопки, встроєної в панель інструментів браузера. Не робить різниці між субдоменами, в результаті – цілий LiveJournal виявляється забанений. Щоб додати виключення, достатньо перезавантажити сторінку і підтвердити необхідність відображення вмісту.

FoxFilter

Плагін, назва якого говорить сама за себе. Контент блокується по набору ключових слів. Користувач може самостійно додавати виключення, якщо заборонена послідовність символів є частиною дозволеної адреси. Розширені можливості настройки надаються за наявності ключа, який є платним

Безпечний Інтернет

ЯК НАЛАШТУВАТИ БАТЬКІВСЬКИЙ КОНТРОЛЬ

Основні поради батькам для онлайн-безпеки дітей:

1. Спочатку комп'ютер бажано ставити в загальній кімнаті, користуватися ним тільки спільно, а дитину треба привчати обговорювати з батьками все, що відбувалося з нею у мережі, і самим ділитися з дітьми власними враженнями від віртуальних занурень.
2. Встановіть **сімейні правила користування Інтернетом**. Беручи до уваги вік дитини, встановіть кілька чітких правил для неї, які передбачають розклад, спосіб підключення та час користування Інтернетом. Дитина має розуміти, що ви довіряєте їй, і ці правила потрібні тільки лише для її безпеки в Інтернеті, а не тому що ви караєте її.
3. **Підвищуйте власну комп'ютерну та інтернет-обізнаність.** Щоб убезпечити свою дитину у Мережі Ви маєте знати про інтернет, принаймні, не менше за неї.
4. **Станьте для дитини порадником. Опановуйте інтернет разом.** Повідомте дитині, що вона може звернутися до Вас у будь-якій ситуації. Якщо в Інтернеті (у повідомленні електронної пошти, на сайті, форумі, чаті) щось не зрозуміло, хвилює або загрожує, дитина завжди має звертатися по допомогу до Вас. Інформація та послуги в інтернеті не завжди безпечні, тому перш ніж завантажувати, копіювати чи встановлювати будь-що з інтернету, дитина має порадитися з Вами. Станьте для своєї дитини другом у соціальних мережах, або попросіть близьких знайомих зробити це. Якщо Ваша дитина не бажає підтверджувати дружбу з Вами, попросіть Ваших друзів молодшого віку подружитися з нею у соціальних мережах. Ви завжди маєте знати, чим займається та з ким спілкується Ваша дитина у Мережі.
5. **Встановіть на мобільному телефоні своєї дитини безкоштовну соціальну послугу «Батьківський контроль».** Регулярно оновлюйте антивірус.
6. **Створіть територію безпечного інтернету.** Використовуйте поновлюваний перелік безпечних для дитини сайтів. Запропонуйте дітям пізнавальні, цікаві та захоплюючі інтернет-ресурси. Щоб захистити дітей від ризиків віртуального світу, використовуйте поновлюваний список рекомендованих сайтів для дітей.
7. **Навчіть дитину правилам безпечної роботи у Мереж**і. Роз'ясніть дитині важливість захисту своєї та чужої конфіденційної інформації:
   - не можна викладати в інтернет інформацію про сім'ю та її фінансові справи,адреси проживання та навчання, номери телефонів, кредитної картки та банківські дані;
   - нікому, крім батьків, не можна називати власні паролі до інтернет-сервісів (навіть найкращім друзям).

   Навчіть дітей поводитися в інтернет так само, як у реальному житті.
8. Створіть вдома територію безпечного Інтернету . Технічні засоби обмеження доступу дитини до небажаного контенту мають використовуватися як дієвий допоміжний інструмент захисту. Існує спеціальне програмне забезпечення для батьківського контролю — на базі операційних систем, антивірусів, а також у вигляді окремих програм — використовуйте їх.

Словничок:

Фішинг — використання інтернет-технологій з метою отримання доступу до конфіденційної інформації про користувачів (паролів, логінів, тощо). Один із прикладів — розсилання електронних листів нібито від імені відомих адресатів із прямим посиланням на спеціально створену фальшиву веб-сторінку.

Грумінг — входження в довіру до дитини з метою схилити її до якоїсь неналежної поведінки, у тому числі й у сексуальному плані.

За допомогою функції **Контроль** на базі **операційних систем**, батьки можуть обмежувати інтервали використання комп'ютера дітьми. Наприклад, можна встановити час, протягом якого діти можуть користуватися комп'ютером. Крім цього батьки можуть обмежувати список програм та ігор, якими може користуватися їх дитина.

Інструкція

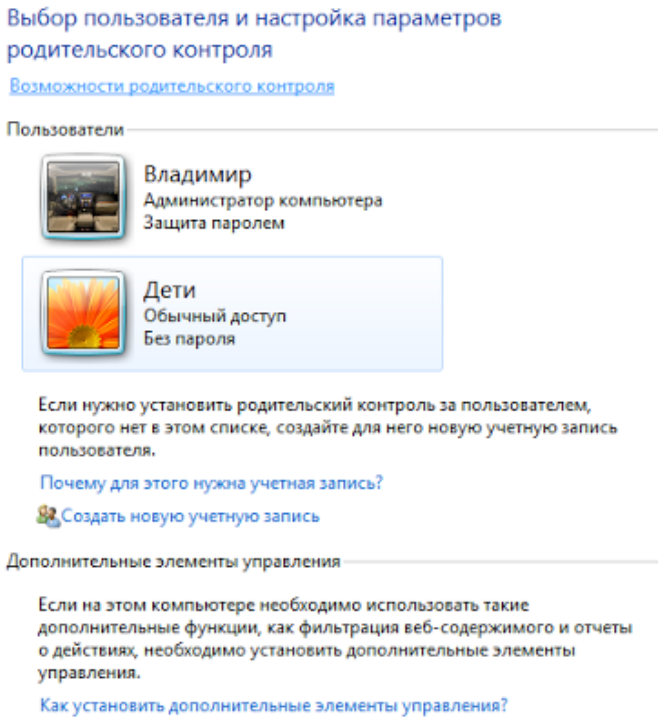
1. Для того, щоб налаштувати батьківський **контроль** , потрібно зайти в кнопку "Пуск". Далі вибираємо "Панель управління" і в розділі "Облікові записи користувачів і безпека" потрібно клацнути по опції "Встановити батьківський **контроль** для всіх користувачів". У відповідь комп'ютер зажадає дозвіл адміністратора. В цьому випадку потрібно або вбити пароль, або відправити підтвердження.
2. Далі потрібно вибрати обліковий запис того користувача, для якого діятиме батьківський **контроль** . Якщо у дитини немає свого облікового запису, то її слід створити для нього і вже стосовно неї використовувати батьківський **контроль** . У групі "Батьківський **контроль** " потрібно вибрати пункт "Увімкнути". Використовуємо поточні параметри. Після того, як все підтверджено, можна починати налаштовувати ті параметри, для яких повинен бути використаний батьківський **контроль** . Наприклад, за часом, або для ігор, або обмеження по відвідуванню інтернету.
3. Дитина, використовуючи комп'ютер, може спробувати зайти туди, де стоїть функція обмеження батьківським контролем. Тоді він може відправити запит батькам дозволити йому доступ. А батьки можуть вирішити варто дати йому послаблення або залишити обмеження без змін.

Російською мовою

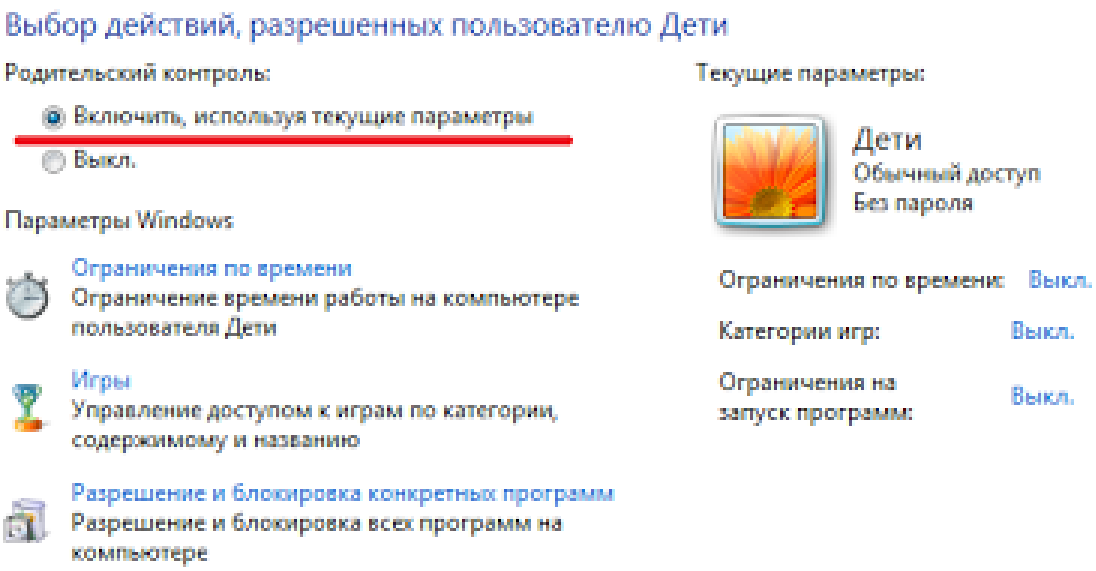
Сделайте для своих детей отдельные учётные записи в операционной системе с соответствующими настройками родительского контроля. При этом, учётная запись администратора должна быть защищена паролем, чтобы ребёнок не мог вносить какие-либо изменения.

Родительский контроль в Windows 7

Для того чтобы установить родительский контроль в Windows 7 жмём: **Пуск** > **Панель управления**. В открывшемся окне, для удобства, выберите просмотр «Мелкие значки» и находим в списке значок **Родительский контроль** – кликаем. На открывшейся странице вы можете увидеть предупреждение, что учётная запись администратора не имеет пароля. Кликаем по ссылке и устанавливаем пароль для администратора. После этого приступаем к созданию учётной записи для ребёнка. В том же окне родительского контроля кликаем по ссылке «*Создать новую учетную запись*» – вводим имя и (если надо) пароль. Последнее, не обязательно, т.к. речь идёт об учётной записи для ребёнка.



Далее выбираем созданную учётную запись для ребёнка и устанавливаем для неё родительский контроль, выбрав **Включить, используя текущие параметры**. Таким образом вы можете настроить ограничения по времени работы ребёнка за компьютером, доступом к играм и программам.



Налаштування безпечного пошуку в Google

Безпечний пошук дозволяє виключати з видачі результатів сайти з матеріалами сексуального характеру. Хоча жоден фільтр не ефективний на 100%, з допомогою безпечного пошуку ви можете захистити себе і своїх дітей від неприйнятного контенту.
За замовчуванням для кожного Інтернет-браузера на вашому комп'ютері встановлена помірна фільтрація, що виключає з результатів пошуку відверті зображення. Якщо ви хочете також виключити непристойний текст, ми рекомендуємо включити режим суворої фільтрації. Параметри безпечного пошуку можна налаштувати, перейшовши за посиланням "Налаштування пошуку" в правому верхньому куті на головній сторінці Google.

Додатки батьківського контролю для Firefox

Наступні додатки можуть бути завантажені та встановлені у Firefox для безпечного перегляду вашими дітьми сайтів в інтернеті. Декілька розширень, що можуть бути необхідні для ваших потреб:

Glubble for Families

Доступний: https://addons.mozilla.org/firefox/ad.../5881 (безкоштовний)
Надає сімейний цікавий перегляд для дітей віком до 12
Glubble дозволяє вам створити приватну сімейну сторінку, де можна контролювати і підтримувати діяльність ваших дітей в інтернеті. Glubble надає ігри, чат, безпечний серфінг, та службу Family Photo Timeline для завантаження, зберігання та обміну фотографіями в інтернеті. Glubble інтегрує безпечний пошуковий засіб для дітей Ask for Kids. Підтримка цього розширення від розробника за адресою http://glubbleparents.ning.com/forum.

ProCon Latte

Доступний: https://addons.mozilla.org/firefox/ad.../1803 (безкоштовний)
Відфільтровує сторінки на основі їх тексту; є можливість керування "хорошим" та "поганим" списком сайтів.
ProCon фільтрує сторінки, використовуючи список недоречних слів та заміняє їх зірочками (***). Враховуйте, що фільтр поганих слів не блокує сайти, що містять ці слова; ви повинні додати сайт до чорного списку. ProCon може також блокувати трафік, і тільки дозволені сайти(встановлені у білому списку) будуть доступні. Ви можете керувати "білими" та "чорними" списками сайтів та сторінок. Також ProCon має парольний захист, щоб не дозволити іншим змінювати налаштування. Підтримка та додаткова документація для цього додатку від розробника за адресою http://procon.mozdev.org/

Безпечний Інтернет

ПЕРЕЛІК РЕКОМЕНДОВАНИХ ДЛЯ ДІТЕЙ ОНЛАЙН – РЕСУРСІВ

затверджений Національною експертною комісією України з питань захисту суспільної моралі

Спеціалізовані Інтернет-сайти дитячої літератури:

- www.childbooks.blox.ua – веб-сайт „Книги для дітей”;
- www.abetka.ukrlife.org – веб-сайт для дітей „Весела абетка”;
- www.abetka-logopedka.org – веб-сайт „Світ дитини”;
- www.kazka.in.ua – веб-сайт „Українська казка”;
- www.ae-lib.org.ua/_lit_child.htm – веб-сайт „Дитяча література”;
- www.levko.info – дитячий сайт „Левко”;
- www.mysl.lviv.ua – веб-сайт „Країна міркувань”;
- www.slovogray.narod.ru – літературний сайт Ігоря Січовика;
- www.dytjachi-virshi.org.ua – авторський сайт „Віршики пана Назара.

Освітньо-інформаційні ресурси:

- http://teacher.at.ua – веб-сайт “Вчитель вчителю, учням та батькам”;
- www.balachka.com – веб-сайт “Пиши українською”;
- http://bibliyna-istoriya.org.ua – веб-сайт “Біблійна історія”;
- http://cikave.org.ua/pro-sajt – веб-сайт “Цікаво про цікаве”;
- http://www.ukr-tur.narod.ru – веб-сайт “Світ географії та туризму”;
- www.akBooks.com.ua – веб-сайт “Академічна книгарня@онлайн”;
- http://lcorp.ulif.org.ua/dictua – український лінгвістичний портал “Словники України”;
- http://www.idea-ukraine.org – проект “Відкритий світ інформаційних технологій”.

Інтернет-сайти бібліотек та електронних бібліотек

- http://www.4uth.gov.ua – веб-сайт Державної бібліотеки України для юнацтва (м.Київ);
- http://www.chl.kiev.ua – веб-сайт Національної бібліотеки України для дітей;
- http://www.nbuv.gov.ua – веб-сайт Національної бібліотеки України імені В.І. Вернадського (м.Київ);
- http://www.bukvoid.com.ua – веб-сайт “Буквоїд”;
- http://www.nplu.org – веб-сайт Національної парламентської бібліотеки України (м.Київ);
- http://www.ukrbook.net – веб-сайт Книжкової палати України імені Івана Федорова (м.Київ);
- http://library.zntu.edu.ua/res-libr-el.html – веб-сайт “Бібліотеки в мережі Internet”;
- http://lyapota.boom.ru/lib.htm – колекція посилань на кращі електронні бібліотеки;
- http://book.uraic.ru/ssylki/biblioteki – інформаційно-довідковий портал “Library.ru”;
- http://www.loc.gov – веб-сайт Бібліотеки Конгресу США;
- www.bnf.fr – Bibliotheque Nationale или BNF) — веб-сайт Національної бібліотеки Франції;
- www.bl.uk – веб-сайт Британської бібліотеки.

Інтернет-сайти світових музеїв та картинних галерей

- http://poklonnayagora.ru – веб-сайт Центрального музею Великої Вітчизняної війни 1941—1945 рр. (Російська Федерація);
- http://www.mmoma.ru – веб-сайт Московського музею сучасного мистецтва (Російська Федерація);
- http://www.polotskmuzey.vitebsk.by – веб-сайт Національного Полоцького історико-культурного музею-заповідника (Республіка Білорусь);
- http://www.palacegomel.by – веб-сайт Гомельського палацово-паркового ансамблю (Республіка Білорусь).

Інтернет-сайти музеїв та картинних галерей України

- http://prostir.museum – портал “Музеи Украины”;
- http://www.prostir.museum/sites/ua – веб-сайт “Музейний простір України”;
- http://namu.kiev.ua – веб-сайт Національного художнього музею України;
- http://www.warmuseum.kiev.ua – веб-сайт Національного музею історії Великої Вітчизняної війни 1941 – 1945 років;
- http://hutsul.museum – веб-сайт Національного музею народного мистецтва Гуцульщини та Покуття;
- http://museum.odessa.net/fineartsmuseum – веб-сай Одеського художнього музею;
- http://www.archaeology.odessa.ua – веб-сайт Одеського державного археологічного музею;
- http://www.oweamuseum.odessa.ua – веб-сайт Одеського музею західного і східного мистецтва;
- http://muzey.vn.ua – веб-сайт Вінницького обласного краєзнавчого музею;
- http://www.museum.lviv.ua – веб-сайт Львівського музею історії релігії;
- http://lvivgallery.org – веб-сайт Львівської національної галереї мистецтв;
- http://honchar.org.ua – веб-сайт Музею І.М. Гончара;
- http://www.chersonesos.org – веб-сайт Національного заповідника “Херсонес Таврійський”;
- http://www.tmf-museum.kiev.ua – веб-сайт Державного музею театрального, музичного і кіномистецтва України.

СПИСОК ДЖЕРЕЛ

1. Ваш особистий Інтернет [Електронний ресурс]. – Електрон. дан. – М., cop. 2008. –
2. Режим доступу: http://www.content-filtering.ru Гончаров Д. К. «Веб — це платформа освіти» зб. «Соціологія ІКТ», М.2010.
3. Безкоштовний фільтр для дітей Інтернет Цензор http://www.icensor.ru/
4. Інтернет ЗМІ «Ваш особистий інтернет» http://www.content-filtering.ru
5. Комплексний освітній ресурс для дітей і вчителів компанії Google та Інтернет Асоціації України http://www.prointernet.in.ua/
6. Центр безпеки Microsoft http://www.microsoft.com/rus/childsafety
7. Центр безпеки Microsoft http://www.microsoft.com/rus/security
8. «Онляндія: моя безпечна веб-країна» http://www.onlandia.org.ua/
9. Національна експертна комісія України з питань захисту суспільної моралі http://www.moral.gov.ua/news/311/
10. Главная - HandyCache - бесплатный локальный кэширующий HTTP прокси-сервер. URL http://handycache.ru/