**НАВЧАЛЬНО-МЕТОДИЧНИЙ ЦЕНТР
ЦИВІЛЬНОГО ЗАХИСТУ ТА БЕЗПЕКИ ЖИТТЄДІЯЛЬНОСТІ
ХАРКІВСЬКОЇ ОБЛАСТІ**

Черепаха В.М., Рачков С.М.

Методичні рекомендації

Питання кібербезпеки та особистого спілкування у віртуальному просторі

Харків

Методичні рекомендації для педагогів освітніх закладів, батьків, дітей та інших зацікавлених у сфері ЦЗ та БЖД.

Автор-упорядник:
Черепаха В.М., методист обласного методичного кабінету
НМЦ ЦЗ та БЖД Харківської області.
Рачков С.М., завідувач обласного методичного кабінету
НМЦ ЦЗ та БЖД Харківської області.

Рекомендовано педагогічною радою
НМЦ ЦЗ та БЖД Харківської області

Протокол № від 2017 року

Дана збірка містить методичні рекомендації, які розкривають поняття кібербезпеки та сприяють виробленню компетенцій у дорослих та дітей щодо безпечного спілкування у віртуальному просторі, уникнення залежності від благ технічного прогресу; виховання поважного ставлення до безпеки людини та її життя.

Зміст

КЛЮЧОВІ ПОНЯТТЯ

Віртуальне спілкування - це спілкування з віртуальним співрозмовником у віртуальному просторі за допомогою електронних засобів.

Кібератака (хакерська атака) - спроба реалізації загрози.

Тобто, це дії кібер - зловмисників (хакерів) або шкідливих програм, які спрямовані на захоплення інформаційних даних віддаленого комп'ютера, отримання повного контролю над ресурсами комп'ютера або на виведення системи з ладу.

Кібербезпека - це процес застосування заходів безпеки з метою забезпечення конфіденційності, цілісності та доступності даних.

Кіберпростір - це віртуальний простір взаємодії, утворений глобальною мережею комп'ютерів, з яких складається Інтернет.

Компетенція - це соціально закріплений освітній результат, здатність (уміння) діяти на основі здобутих знань

Нетикет - («netiquette»; від англ. network etiquette) –це правила поведінки, спілкування, традицій у мережі Інтернет.

Вступ

Інтернет (Internet) - глобальна комп'ютерна мережа, яка відкрила нові види взаємодії - "людина-комп'ютер" та "людина-комп'ютер-людина"- і дає безмежні можливості для комунікацій та діяльності всьому людству. Інтернет має близько 15 мільйонів абонентів у більш ніж 150 країнах світу, причому щомісяця розмір Мережі збільшується на 7-10 відсотків. Мережа Інтернет утворює ядро, що забезпечує зв'язок різних інформаційних мереж, що належать різним установам у всьому світі. Одним словом, Інтернет являє собою повноцінне джерело різноманітної корисної інформації для всіх, а також стає основною формою віртуального спілкування.

Спілкування як явище - є спосіб взаємодії людей один з одним, а з появою всесвітньої павутини це спілкування вийшло за рамки одного будинку, міста і навіть однієї країни. Безперечно, багато років існували й інші засоби передачі інформації на відстані (такі як пошта, телефон, телеграф), але ті незручності, з якими часто стикаються учасники такого спілкування, змушують багатьох з них перейти в ряди тих людей, хто вже оцінив переваги нового світу цифрових технологій і зокрема Інтернету. На сьогодні електронна пошта, всілякі форуми, організовані в мережевому просторі, численні Інтернет - журнали і газети, та й сам Інтернет для багатьох стали не менш важливим аспектом повсякденності, ніж телевізор або телефон, а часом вони і повністю витісняють своїх «відсталих» братів.

У мережевої комунікації є маса переваг у порівнянні з загальноприйнятими способами особистого спілкування, недаремно її і називають «всесвітня павутина»: вона, охоплюючи майже всі цивілізовані куточки нашої планети, є потужним засобом міжкультурного контакту, сприяє зближенню народів і зростанню їх національної та міжнаціональної самосвідомості.

Та щоб не потрапити в буквальному сенсі в згубне павутиння, слід кожному, а особливо молоді, знати, які загрози несе Інтернет і як їх слід уникати.

Володіння такими знаннями, вміннями та будь-якими навичками чи способами дій визначається як кіберкомпетенція.

Вивчення рекомендацій, правил та порад, викладених в даній збірці, - це шлях вироблення необхідних компетенцій для здійснення продуктивної та безпечної життєдіяльності у кіберпросторі.

I
Кібербезпека: захисти себе сам

Протягом останнього року на сотні українських підприємств, організацій та установ були здійснені хакерські атаки, остання з яких - модифікована версія вірусу wannacry – cryptolocker – «Petya» спричинила величезний збій системи у мільйонів українців.

Організатори атаки добре знали специфіку розсилок службових листів і тому маскували розсилання вірусу під ділове листування, яке через цікавість відкривали малодосвідчені користувачі. Після появи перших симптомів багато хто з користувачів перезавантажували комп'ютери, тим самим запускаючи вірус, який зашифровував всі дані жорсткого диску та вимагав викуп в декілька сотень доларів (з сайту:http://comments.ua/tema/Facebook.html").

Навчити користувачів комп'ютерів уникати таких кібератак та запобігати їх наслідкам покликана кібербезпека.

Кібербезпека - це процес застосування заходів безпеки з метою забезпечення конфіденційності, цілісності та доступності даних.

Іншими словами, це рівень захищеності домашнього комп'ютера чи приватного веб-сайту від зламу хакерами.

Користувачі не можуть попередити можливу загрозу в мережі чи поза нею, але в їхніх силах можливість мінімізувати ризики за допомогою деякої обережності та здорового глузду.

Безумовно, будь-який захист починається з усвідомлення того, чого потрібно остерігатися.

Ось короткий виклад трьох найбільш типових загроз кібербезпеки:

1. Маніпуляція.

Підступні хакери використовують всі види обману для отримання доступу до вашої особистої інформації та її використання. Основними з яких є:

- Фітинг (шахрайська діяльність, метою якої є отримання доступу до конфіденціальної інформації користувача (логінів, паролів);
- спам;
- зламані облікові записи;
- класичний лист "Принца Нігерії" (також відомий як "шахрайство 419").

2.Зловмисне програмне забезпечення.

Це небезпечні маленькі програми, створені для зараження вашого комп'ютера з метою його пошкодження, викрадення особистої інформації, шпигунства чи показу реклами - віруси, черв'яки, Троянські програми…

3.Мережеві та комп'ютерні атаки.

Веб - сайти й мережі вразливі до атак, як до простих, так і до достатньо вишуканих. Такий вид загрози найважче попередити, але можливо встановити додаткові бар'єри.

Для уникнення потрібно:

1. Довіритися власній інтуїції.

Якщо ви відчуваєте, що посилання чи завантаження виглядає неправильно, швидше за все так і є. Переконайтеся, що ви встановлюєте програми лише з перевірених довірених джерел, а також не натискайте на будь-що, якщо воно виглядає хоча б трохи підозріло – навіть якщо ви вважаєте, що ви знаєте джерело.

2. Остерігатися публічного доступу.

Коли ви користуєтеся Інтернетом в загальнодоступній мережі Wi-Fi, будь-хто може перехопити деяку або всю вашу діяльність. Тому уникайте виконання ненадійних дій при публічному доступі. А також перед тим, як ділитися будь-якою інформацією в мережі, подумайте про те, як вона може зробити вас вразливими.

3. Використовувати надійні паролі та двоетапну авторизацію.

Надійні паролі та PIN-коди - це ваш єдиний найкращий захист проти майже кожного виду загрози в Інтернеті. Створюйте надійний пароль для кожного пристрою і облікового запису. І візьміть собі звичку змінювати свої паролі раз на рік - не використовуйте один пароль всюди.

Для найкращого захисту користуйтеся перевагами двоетапної авторизації там, де вона пропонується.

4. Встановити систему безпеки, яка попереджає і захищає від кіберсюрпризів:

- антивірусне програмне забезпечення: воно не захистить від усього, але це хороший початок: наприклад, AVAST…

- додатки Firefox – вони допоможуть вам визначити те, на що ви збираєтеся натиснути мишею:

- Long URL please — замінює більшість скорочених URL- адрес на оригінальні, щоб ви знали повний шлях.

- URL Tooltip — показує шлях посилання при наведенні над ним курсора миші.

Пам’ятайте, сайт є безпечним в тому випадку, коли його адреса починається з **https.**

Кібербезпекою в Україні офіційно займається Департамент кіберполіції, тому при будь-яких підозрах на шахрайство та загрозах слід повідомляти на

сайт: **https://www.cybercrime.gov.ua** (цілодобово), або дзвонити на телефон гарячої лінії: **(044) 374-3758** (з 8:45 до 18:30 в робочі дні).

II
Безпека дітей в Інтернеті

Інтернет - технології стали природною складовою життя дітей і сучасної молоді. Комп'ютер є не тільки розвагою, але й засобом спілкування, самовираження та розвитку особистості.Самостійне пізнання інформаційного світу дозволяє розширити коло інтересів дитини і сприяє її додатковій освіті, спонукає до кмітливості, привчає до самостійного розв'язання задач. Всесвітня мережа також задовольняє потребу підлітків у лідерстві. Діти, які добре знають комп'ютер та Інтернет, більш адекватно оцінюють свої здібності та можливості, вони більш цілеспрямовані та кмітливі. Щоб повноцінно орієнтуватись у віртуальному просторі, дитині треба вчитися структурувати великі потоки інформації, дотримуючись основних правил безпеки в мережі.

Всеукраїнське соціологічне дослідження, проведене Інститутом соціології НАН України в 2009 році, виявило тривожні тенденції: понад 28% опитуваних дітей готові надіслати свої фотокартки незнайомцям у Мережі; 17% без коливань діляться інформацією про себе і свою родину (адреса, професія, графік роботи батьків, наявність цінних речей у домі тощо); 22% дітей періодично потрапляють на сайти для дорослих; 28% дітей, побачивши в Інтернеті рекламу алкоголю або куріння, хоча б один раз спробували їх купити, а 11% − спробували купувати наркотики; близько 14% опитуваних час від часу відправляють платні SMS за бонуси в онлайн - іграх і лише деякі звертають увагу на вартість послуги. Лише у 18% випадків дорослі перевіряють, які сайти відвідує дитина, тільки 11% батьків знають про такі онлайн - загрози, як "дорослий" контент, азартні ігри, онлайн - насилля, кіберзлочинність.

Інтернет - загрози виділяють в чотири види, а саме:

І.Загрози фізичному благополуччю:

1. Виникають від довготривалого сидіння за комп'ютером:

- астенопатія, біль в спині, шиї, зап'ястний синдром,епілепсія, тенденіти, стенокардія, висипи на шкірі обличчя, хронічний головний біль, запаморочення…
- синдром комп'ютерного стресу - це поява порушення пам'яті, безсоння, погіршення зору, головний біль, хронічна втома, депресійний стан, проблеми у спілкуванні…

2. Як наслідок використання Інтернету:

- зниження концентрації уваги;
- порушення сну;
- зустріч з незнайомцями з мережі;
- педофілія;
- пропаганда психоактивних речовин, заклики до масового вживання наркотиків;

- зневага харчуванням;
- заподіяння собі чи іншим шкоди, суїцид тощо.

2. Загрози психічному благополуччю:

- розповсюдження особистих даних в Інтернеті,

порушення конфіденційності та онлайн -недоторканності приватного життя;

експлуатація довіри;

кіберагресія, кібербулінг, залякування;

- розпалювання ненависті та нетерпимість, мова ворожнечі, тролінг;
- зміст порнографічного або сексуального характеру, секстинг, Інтернет-повідомлення інтимного змісту;
- жорстокі та азартні ігри;
- приниження почуття гідності, порушення прав людини;

низька якість інформації та інформаційне перевантаження тощо).

3. Загрози соціальному благополуччю:

- підвищена збудженість;
- депресивні стани;
- перешкода для виконання домашніх справ;
- зменшення часу спілкування в реальному світі;
- залежність тощо;

4. Загрози матеріальному благополуччю:

- реклама, спам, віруси;
- незаконні завантаження;
- азартні онлайн ігри;
- кібератаки, кібертероризм;
- придбання товару низької якості;
- втрата коштів;
- пошкодження програмного забезпечення комп'ютера;
- піратство;
- Інтернет-злочинність, Інтернет-шахрайство;

-різні форми Інтернет- маркетингу, матеріальні збитки**.**

Основна рекомендація, що гарантує безпеку дитини в інтернеті - довірче спілкування з батьками. Дитина повинна знати, що головні експерти у всіх життєвих ситуаціях — її мама й тато. Не повинно бути таких тем, які дитина боялася б обговорювати з батьками й питань, які дитина посоромилася б поставити. На жаль, у багатьох родинах довірчі відносини втрачені, і батьки з дітьми живуть поруч, але не разом.

Якщо такі проблеми є , дані рекомендації зможуть відновити довіру у вашій родині.

І. Хоча б 15 хвилин у день спілкуйтеся з дитиною так, щоб ви дивилися одне одному в очі.

Але тільки не тоді, коли ви її лаєте! Контакт «очі в очі», повинен асоціюватися в дитини тільки з теплим, довірчим спілкуванням.

ІІ. Починайте й закінчуйте день разом.

Будіть дитину вранці, нехай вона бачить ваш гарний настрій. Намагайтеся, у міру її віку, укладати її спати. Навіть діти 7 років люблять казку на ніч, а для дітей старше важлива щиросердечна бесіда.

ІІІ. Враховуйте вікові особливості дитини:

1. Дитині до 7 років цікаво й навіть необхідно грати, особливо у розвиваючі й сюжетно-рольові ігри. Чому б не надавала перевагу дитина - віртуальним іграм або іграм з батьками й іншими дітьми, - усе буде корисно для її розвитку, якщо дотримуватися обмежень за часом. Інакше віртуальні ігри можуть швидко стати для маляти сенсом життя, а реального спілкування дитина буде уникати. Відводьте на віртуальні ігри півгодини в день, а на ігри з однолітками — 3- 4 години.

2. З 7 до 11 років діти як і раніше полюбляють грати й прагнуть використати інтернет саме як майданчик для ігор. Але в цьому віці в дітей прокидається соціальне «Я». Дітям важливо зайняти значуще місце в житті свого маленького світу: класу, школи, дружити з однолітками. Тут їм буде потрібна реальна допомога й проста увага батьків. Перші невдалі спроби дружби в початковій школі можуть травмувати дитину. У цьому випадку батьки зможуть дати їй практичні поради зі встановлення контакту з однолітками, разом беручи участь у віртуальному спілкуванні в мережі. Зрозуміло, у всьому необхідно дотримуватися міри, і тоді інтернет стане дитині помічником у подоланні бар'єрів спілкування, партнером у розвиваючих іграх, учителем у вивченні іноземних мов, джерелом необхідної інформації для уроків і просто — музики, картинок і фотографій, мультфільмів і позитивних емоцій.

3. Дитина в 11-14 років - це підліток. І найголовнішою, значущою, провідною її діяльністю є спілкування з ровесниками. Тут Інтернет може стати просто незамінним помічником. Але, знову ж, все добре в міру! Інтерактивне спілкування потрібно обов'язково сполучати з реальним. Після 11 років у підлітків уже починає активно прокидатися інтерес до питань дорослого життя, психології статі і всього, що із цим пов'язане. Важливо, щоб відповіді на свої питання підліток знаходив у першу чергу в батьків, а не на сумнівних сайтах. Крім того, у цьому віці в дітей з'являються кумири: співаки, спортсмени й артисти, про які їм хочеться довідатися все. У цьому

випадку Інтернет - кращий помічник і інформатор. Але батькам потрібно бути пильними, адже зірок найчастіше супроводжує скандальна інформація.

4. Дитина старше 14 років — уже досить доросла людина і вважає, що сама краще знає, як їй треба поводитися, яку музику слухати, що читати, з ким спілкуватися. Цікавтеся всім тим, чим цікавиться ваша дитина, намагайтеся вникнути в коло її інтересів і спілкуйтеся з нею про них, навіть якщо це «не ваша тема». Починаючи із цього віку, з дитиною можна говорити й про вибір майбутньої професії. А в Інтернеті можна знайти безліч інформації, що допоможе дитині визначитися, а вам - контролювати й, якщо буде потреба, коректувати вибір дитини, знаходячи більше повну інформацію про переваги й про недоліки різних професій.

В цій віковій категорії у дитини існує ризик стати Інтернет - залежною. До залежності найбільше схильні діти, у яких не складаються відносини з однолітками й батьками, які намагаються віднайти заміну живому спілкуванню у віртуальних іграх і чатах. Тут, у розмові з дитиною важливо не протиставляти Інтернет реальному життю, а показати як вони можуть доповнювати одне одного. Наприклад, якщо ваша дитина занадто захоплена іграми - стрілялками, запропонуєте їй стати сильним героєм не тільки на екрані мобільного телефону або монітора, а насправді зайнятися спортом, навчитися прийомів самооборони й т. д. Сходіть разом у спортзал, знайдіть підходящу спортивну секцію.

Щоб не допустити комп'ютерну залежність, потрібно знати:

1. Симптоми:ейфорія під час роботи за комп'ютером, неможливість зупинитися, збільшення часу перебування в Інтернеті, відчуття тривоги, роздратованість поза комп'ютером, порушення сну, зневага до гігієни.

2. Предвісники: нав'язливе бажання постійно перевіряти електронну пошту,очікування чергового сеансу онлайн, зростання витрат на Інтернет - послуги.

3. Ознаки:

- пропуски шкільних занять через комп'ютерну гру вдома або відвідування комп'ютерного клубу;
- просиджування біля комп'ютера у нічний час;
- приймання їжі під час комп'ютерної гри;
- асоціювання себе з героями комп'ютерних ігор;
- відсутність інших захоплень, крім комп'ютерних ігор;
- віддавання переваги комп'ютерним іграм, а не спілкуванню;

- загальний час, проведений за грою, перевищує час виконання домашніх завдань, прогулянок, спілкування з батьками й однолітками, інших захоплень;

- дитина не уявляє, чим себе зайняти, коли комп'ютер не працює;

- конфлікти з батьками та їх шантажування у відповідь на заборону проводити час за комп'ютером.

4.Стадії залежності:

I - Стадія легкого захоплення – віддалення від сім'ї, приховування часу, що проводе в Інтернеті.

II - Стадія захоплення – бажання грати в комп'ютерні ігри, при відлученні від комп'ютера переживає муки наркомана.

III - Стадія соціальної дезадаптації: соціалізована форма – постійно "зависаючи" на сайтах не одержують задоволення від спілкування; індивідуалізована форма – стан депресії та конфлікти – потреба у фахівцях.

5. Профілактику комп'ютерної залежності у дітей:

1. Привчайте дитину правильно ставитися до комп'ютера, як до технічного пристрою, за допомогою якого можливо отримати знання і навички, а не як до засобу отримання емоцій.

2. Не дозволяйте дитині у віці 3-5 років грати у комп'ютерні ігри.

3. Розробляйте з дитиною правила роботи за комп'ютером: 20 хв. комп'ютерної гри, ЗО хв. - інші види діяльності.

4. Не дозволяйте дитині їсти і пити біля комп'ютера.

5. Не дозволяйте дитині грати в комп'ютерні ігри перед сном.

6. Домовляйтеся з дитиною виконувати ці правила.

7. Обговорюйте з дитиною покарання у разі, якщо вона порушить домовленість.

8. Коли дитина дотримується ваших вимог, обов'язково скажіть їй про свої почуття радості чи задоволення. Таким чином закріплюється бажана поведінка.

9. Не використовуйте комп'ютер як засіб для заохочення дитини. Під час хвороби і вимушеного перебування вдома комп'ютер не повинен стати компенсацією.

10. Допомагайте дитині долати негативні емоції, які бувають у житті кожної людини (розчарування, сум, образа, агресія тощо) і які можуть підштовхнути її отримати полегшення за грою.

IV. Розвивайтеся з Інтернетом.

Розмовляйте з дитиною про те, що нового й цікавого вона довідалася з Інтернету. Але спочатку - розповідайте, що важливого й корисного Ви робите з його допомогою самі. Разом з дитиною знаходьте в Інтернеті відповіді на питання, що її цікавлять. Навчить її, як за допомогою Інтернету можна уникнути складних ситуацій, наприклад, не заблукати в незнайомому місці, використовуючи карти; як знайти необхідну інформацію або одержати пораду. Покажіть їй, скільки цікавого і корисного можна знайти в мережі. Але показуючи дитині багатогранність Інтернету, не забудьте розповісти про правильне ставлення до нього. Наприклад, можливість онлайн - спілкування із другом, що живе далеко - це одна із чудових можливостей мобільного Інтернету, а от спілкування винятково з віртуальними друзями - це вже крайність.

V. Зберігайте фізичне здоров'я дитини: дотримуйтесь часових норми неперервного перебування за комп'ютером (згідно нормативів Міністерства охорони здоров'я України)

Впродовж доби: 1-2 клас – 10 хв;

3-5 клас – 15хв.;

6-7 клас -20хв.;

8-11 клас – 30хв.

(максимально 2 години з 10 хв.перервою)

На тиждень: 1 клас – 30-40хв.;

2 -3 клас – 2 години;

4-6 клас – 2 години;

7-9 клас – 2, 5 години;

10-11клас – 7 годин.

(не більше 1 години на добу).

VI. Пам'ятайте про те, що дитина може мати доступ до небажаного контенту (порнографія, пропаганда наркотиків,психотропних речовин,алкоголю, тероризм та екстремізм, ксенофобія, сектанство, асоціальна поведінка, агресія,азартні ігри, Інтернет - шахрайство…):

1. Дитина емоційно не готова сприймати відверті матеріали щодо статевих відносин, які можуть завадити формуванню нормальної сексуальної та громадської поведінки.

2. Негативний вплив на уяву про здорові сексуальні стосунки.

3. Нівелювання сімейних цінностей.

4. Ранній початок інтимного життя.

5. Може стати жертвою злочинців, педофілів та збоченців.

6. Перегляд матеріалів зі сценами насильства перешкоджає нормальному формуванню моральних цінностей.

Можливі наслідки

1. Розкритя конфіденційної інформації.

2. Кіберкомунікативна залежність.

3. Кіберсексуальна залежність (потяг до сексуальних обговорень та сайтів).

4. Секстинг - фотографування себе оголеними і пересилка знімків.

5. Кібербулінг - переслідування дітей, залякування.

6. Кібергрумінг - входження в довіру до дитини з метою сексуального використання.

7. Виробництво та розповсюдження дитячої порнографії.

8. Шахрайство: “ Передзвони мені!” (знімають кошти).

9. Фішин та вішинг - крадіжка особистих даних.

10. Фармінг - зараження вірусами.

VII. Вивчіть разом з дітьми наступні правила безпеки в мережі:

- не спілкуватися у мережі з незнайомцями та не додавати їх в друзі – батьки обов'язково повинні значитися в друзях;

- не викладати відверті фотографії, призначені тільки для близьких людей;

- не повідомляти свої геоданні, відключати служби геолокації в додатках;

- не виставляти у вільний огляд: домашню адресу (у тому числі не варто робити фото на тлі табличок будинків), номер телефону, фото документів, на яких можна розгледіти паспортні дані (в тому числі і квитки), номерні знаки батьківських машин;

- дотримуватися приватності в чатах, пам'ятати, що твої повідомлення може прочитати чужа людина;

- не світити на фото і відео дорогі подарунки і покупки батьків;

- зробивши дурість в мережі – признатися батькам.

III
Особливості спілкування у віртуальному просторі

За дослідженнями спеціалістів метою потрапляння в кіберпростір є:

- навчання і розвиток: опрацювання навчальних наукових матеріалів, читання новин, підвищення рівня знань технічної та медійної освіченості, опанування роботи з комп'ютером в Інтернеті;

- розваги: гра, слухання музики, перегляд фільмів та відеороликів;

- спілкування: знайомство і пошук нових друзів, участь у дискусіях і віртуальних форумах, чатах тощо…

91% користувачів використовують Інтернет саме для спілкування.

Електронна пошта перетворила віртуальне спілкування на силу, яку не можна не враховувати. Вже через 30 днів після відкриття, без будь-якої реклами та публікацій у пресі, «Amazon.com» продавав книжки у всіх штатах Америки та 45 інших країнах світу. Для цього керівник фірми Джефф Безос лише надіслав електронні листи своїм 300 друзям і попросив їх розповісти про новий сайт своїм знайомим. Тільки за останніх два роки відсоток користувачів Інтернету в Україні виріс більше ніж у півтора рази. Нині всесвітньою павутиною в країні користується 5 млн. населення.

Багато організацій в Інтернеті надають можливість доступу до інтерактивних сервісів, які підтримують «живу» бесіду між мешканцями різних міст, країн або спільнот. Створено програми, які підтримують «живе» спілкування в режимі реального часу. Наприклад, у телеконференції за допомогою електронних засобів спілкування беруть участь великі групи користувачів. Існують і локальні телеконференції, які присвячуються конкретним подіям або чітко визначеній темі. У конференції спілкування відбувається навколо певної теми, тоді як чат, як правило, визначеної теми не має. Спілкування у деяких програмах можна вважати аналогом телефонної розмови. При цьому дві особи, які спілкуються, мають доступ до одного серверу і знаходяться у системі в той самий час. Кожен із співрозмовників має змогу відразу ж бачити все, що набирає на клавіатурі свого комп´ютера його партнер. І хоча вони не бачать і не можуть уявити один одного, але передають свої думки, емоції, обмінюються інформацією й одночасно реагують на неї.

Спілкування в Інтернеті має певні особливості:

1.Наявність особистого простору, в який нікому немає доступу.

Спілкуючись в Інтернеті, можна створювати будь-який образ, виглядати ким завгодно, бо немає обмежень, характерних для матеріального світу.

2.Анонімність.

Анонімність розширює можливості для само презентації людини, дає змогу створювати іншим яке завгодно уявлення про себе. У цьому контексті

навіть можна говорити про «віртуальну особистість». Вона наділяється іменем, часто псевдонімом, а її реальне «Я» дуже відрізняється від створеного віртуального образу. Крім того, взаємодія тут має свої особливості, а саме: попередню невизначеність; унікальність для кожного роду взаємодії; а також існування тільки протягом самої взаємодії.

3. Відсутність відповідальності - розмиваються рамки загальноприйнятих понять: добре / погано, пристойно / непристойно, красиво / вульгарно тощо.

Інтернет - це середовище, в якому декларується абсолютна свобода, повна демократія, тут кожний має право голосу і доступу до інформації. А якщо це так, то деякі вважають за можливе робити в Інтернеті все, що завгодно, тим паче, що ці дії можуть бути анонімними. Такий характер спілкування у віртуальному середовищі певним чином нівелює систему традицій, правил, цінностей, що склалися історично і характеризують належність особистості до будь-якої співдружності, як-то: нація, клас або релігійна конфесія. Тут не можна жестикулювати, змінювати тон. Тільки слова бачать на екрані співрозмовники. Коли ведеться розмова електронною поштою або в конференції, можна дуже легко помилитися в тлумаченні слів співрозмовника. На жаль, під час розмови у віртуальному просторі іноді забувається про те, що адресат теж людина зі своїми почуттями і звичками.

4.Реалістичність процесів та повне абстрагування від навколишнього світу.

5.Добровільність і бажаність контактів - контакти швидко зав'язуються і перериваються у будь-який момент.

Коли хто-небудь надсилає повідомлення в Інтернет, його можуть читати всі і відповідати на нього. Можна приєднатися до чужої розмови, а можна розпочати свою, а можна не відповідати взагалі.

6.Можливість виправити будь-яку помилку шляхом багаторазових повторень.

7.Можливість самостійно приймати рішення незалежно від наслідків.

В зв’язку з цим існує небезпека: інформація, яка передається у віртуальний простір, фіксується і може зберегтися, а потім повернутися і зашкодити тому, хто її надіслав, і вплинути на цей процес можливості вже не буде.

8. Можливість отримувати інформацію та вчитися її «фільтрувати», що позитивно впливає на логічне мислення, пам'ять, увагу.

9. Втрата емоційного розвитку: людина не розвивається, адже текстові повідомлення позбавлені міміки, жестів, енергетичних імпульсів.

10. Набуття проблеми самоідентифікації: зникають обмеження у власній презентації, з'являється прагнення до нетипового, ненормативного у поведінці(можна стати розумним, дотепним, популярним і гарним тощо…).

11. Вироблення своєрідності протікання процесів міжособистісного сприйняття в умовах відсутності невербальної інформації - включаються механізми стереотипізації, ідентифікації, установки бажаних якостей у співрозмовника.

1. Етикет у віртуальному спілкуванні

Віртуальне спілкування має свою віртуальну структуру, свої правила і навіть свої традиції. Тут спілкування відбувається у режимі реального часу, як у разі «живої розмови», але за допомогою клавіатури. Але те, про що говорять двоє людей, можуть бачити і читати десятки інших. На жаль, підключившись до якогось каналу, можна прочитати будь-яку дурницю, хуліганські вислови тощо. Водночас людина, яка поважає себе та інших, і в тому середовищі, де ніхто її не бачить, спілкуючись з іншими, спиратиметься на етичні цінності, норми та принципи, які в мережі Інтернет мають назву нетикет.

Нетикет - («netiquette»; від англ. network etiquette) – це правила поведінки, спілкування, традицій у мережі Інтернет.

Правила нетикету встановлюють користувачі мережі. Так само, як і в реальному світі, у віртуальному теж повинні бути свої правила етикету. Саме від того, який відсоток користувачів дотримується правил віртуального спілкування, залежить зручність існування в мережі всіх інших.

Єдиного документу, що відображає усі правила мережевого етикету і є стандартом для усіх,досі не існує. Але існують найбільш поширені правила, які повинен знати кожен інтернетівець:

Правило 1. *Пам'ятайте, що ви спілкуєтесь з людиною.*

Досить часто люди в мережі порушують дане правило,забуваючи, що по той бік екрану з ними спілкується жива людина. Не зловживайте тим, що співрозмовник вас не бачить і не дозволяйте собі того, чого б не зробили у звичайному спілкуванні. У віртуальному світі є таке поняття як тролінг, що являє собою провокаційні повідомлення, які пишуться деякими особами (тролями) з метою викликати конфлікт між учасниками спілкування. Тому, заради свого спокою,уникайте конфліктних ситуацій та не провокуйте їх. Пам'ятайте, що не потрібно робити для інших те, чого не хочете щоб зробили для вас.

Правило 2. *Дотримуйтеся тих самих стандартів поведінки, що і в реальному житті.*

У віртуальному світі існує певне відчуття анонімності, і в деяких ситуаціях люди можуть дозволити собі більше, ніж вони дозволяють,спілкуючись у реальному житті. Але, все ж таки, намагайтесь дотримуватись правил спілкування, як в реальному, так і у віртуальному спілкуванні. Залишайтесь толерантними і пам’ятайте, що Інтернетом користуються і діти.

Правило 3. *Пам'ятайте, що ви знаходитесь у кіберпросторі.*

Активне спілкування у мережі має свої нюанси. Так, спілкуючись в чаті або на форумі, пам’ятайте, що манери спілкування в різних співтовариствах різні. Якщо один стиль спілкування цілком звичний для одного

співтовариства, для іншого він буде абсолютно неприйнятним. Обов'язково, перед тим як щось коментувати в цілком новій для вас темі, озирніться, вивчіть обстановку –послухайте про що і як говорять там люди, і лише після цього долучайтесь до розмови. Не варто нав'язувати свої правила і вчити співтовариство, навіть якщо ви впевнені, що всі не праві.

Правило 4. *Поважайте час і можливості інших.*

Якщо ви хочете поділитись з усім світом важливою для вас новиною, подумайте, чи всім вона така корисна. Одним з наслідків цього правила є шанобливе ставлення до чужого трафіку. Відправляючи кому-небудь надмірної ваги файл, користуйтеся архіватором. Викладаючи великі зображення, подбайте про те, щоб їх супроводжували невеликі прев'ю (від preview – попередній перегляд зображення, як право, в зменшеному вигляді) із зазначенням розміру файлу. Якщо ви даєте посилання на великий файл, не забувайте вказувати його розмір. Не слід очікувати миттєвої реакції на повідомлення.

Правило 5. *Зберігайте свій імідж.*

Ваша репутація в Інтернеті не менш важлива, ніж у реальному житті. Навіть якщо здається, що ніхто в Мережі вас не впізнає, не варто ображати інших, створювати конфліктні ситуації,або відповідати на образу образою. Нехай друзі за інтересами та сайтами знають вас як ввічливу, толерантну та порядну людину. Публікуючи якусь інформацію, перевірте її достовірність, пишіть грамотно.

Правило 6. *Допомагайте іншим там, де ви це можете зробити.*

Мережа не є сховищем всіх можливих у світі знань. Зазвичай в Інтернеті з'являється лише та інформація, яка несе вигоду її автору. Досить часто у людей виникають запитання, на які в мережі відповіді немає, тому, якщо ви є компетентні в якомусь питанні і можете на нього відповісти – відповідайте. Якщо ви виявили, що в Інтернеті відсутня інформація про щось, що ви знаєте напевне – обов'язково напишіть про це: ваші знання можуть комусь знадобитись. Якщо в Мережі вас просять допомогти – допоможіть, можливо хтось колись так само допоможе вам.

Обмінюйтесь досвідом у мережі, адже сам Інтернет виріс завдяки бажанню людей ділитись інформацією.

Правило 7. *Не створюйте конфлікти та не допускайте їх.*

«Словесну війну», яка іноді виникає між декількома учасниками дискусії, ще називають флеймом (від англ. flame —полум'я). Зазвичай, під час таких суперечок істина не народжується і виникає лише дискомфорт серед учасників обговорення. Інтернет не забороняє флейми, вони можуть нести задоволення як авторам, так і читачам, а ті, хто їх отримує, цілком можуть на них і заслуговувати. Проте, нетикет не заохочує таких дій, які

іноді переростають у справжні інформаційні війни. Краще уникайте образ і не беріть участі у конфліктних обговореннях.

Правило 8. *Поважайте право на приватне листування.*

Як і в реальному, так і у віртуальному світі існує право особи на приватне листування, і неповага до цього права – ознака поганих манер. Інколи у виникають моменти, коли користувачі не виходять зі своїх сторінок у соціальних мережах та електронної пошти, або просять когось відкрити їх скриньку і роздрукувати якусь інформацію. Цій особі потрібно обов'язково попередити людину про можливі ризики, показати,як самостійно відкрити скриньку та порадити користувачеві не довіряти нікому свій пароль і вводити його самостійно.

І запам'ятайте ще один момент, який також відносять до даного правила: не поширюйте в мережі інформацію про себе та інших людей – реальні імена, адреси, телефони, фотографії!

Правило 9. *Пам'ятайте про авторське право.*

Ні в якому разі не привласнюйте собі чуже авторство! Представляти скопійовану з Інтернету інформацію як авторську не просто нечесно, але й незаконно. Зверніть увагу й на те, що завантажувати і поширювати фото, відео та музику, які захищені авторським правом теж не варто (звісно, якщо попередньо ви не здійснили оплату копійованого матеріалу), адже це прирівнюється до крадіжки. Публічні установи повинні поширювати серед своїх користувачів знання авторського права.

Правила 10. *Пам'ятайте про безпеку.*

Намагайтесь без зайвої потреби не викладати на сторінках мережі приватну інформацію, щоб не стати жертвою он-лайн злочинців. Якщо все-таки така потреба виникла, перед тим, як написати щось про себе, обов'язково перевірте безпечність сайту. Сайт є безпечним в тому випадку, коли його адреса починається з https разі виникнення в Інтернеті ситуацій, які порушують безпеку комп'ютера або вашу безпеку особисто(листи з погрозами тощо),повідомте про це компетентну особу.

Для того,щоб усім користувачам Інтернет - мережі було комфортно нею користуватись потрібно усвідомити, що Інтернет – це не «дика» зона, яка не має правил. Саме загальнолюдські цінності впливають на якісне формування змісту ресурсів і послуг цієї зони, і саме від її користувачів залежить,як вони будуть співіснувати в ній, незалежно від національності, культурних та релігійних поглядів.

2. E-mail – етикет

Електронна пошта — це досить зручний спосіб швидкого та ефективного спілкування. Звісно, електронна пошта не є найкращим способом передачі конфіденційної чи делікатної інформації та позбавлена важливих елементів спілкування – виразу обличчя, жестикуляції, поз, інтонацій голосу, але є, безумовно, одним з найкращих способів для професійного, ділового спілкування. Проте, щоб залишити після свого листа гарне враження про себе,особисто потрібно знати елементарні правила етикету спілкування в електронній пошті.

Адреси та персональні імена

Персональне ім'я (не те ж саме, що підпис) – це довільний рядок, який більшість програм електронної пошти (мейлери) дозволяють приєднувати до ваших повідомлень в якості текстового коментаря.

Якщо ваша система дозволяє, завжди пишіть персональне ім'я: воно є для вас кращою «візитною карткою», ніж просто адреса e-mail.

Використовуйте осмислені імена. Адреса повинна мати ім’я та прізвище, щоб можна було визначити автора листа. Не використовуйте виразів, які схожі на ніки або прізвиська, наприклад: «здогадайся сам», «luceenok134», «ромашка» тощо. Це заважає визначити авторство листа, а також ображає адресата. Вирази даного типу не лише заважають визначити автора листа, а й ображають інтелект адресата.

Тема листа

(Subject) Перед відправленням,обов’язково вказуйте тему листа. Майже всі мейлери мають можливість присвоєння електронним листам назви, і найчастіше будь-який користувач орієнтується саме по назвах при перегляді своєї пошти.

Уникайте безглуздих назв. Наприклад, відправляючи лист службі підтримки Microsoft, не слід давати йому назву Microsoft –з цим же успіхом ви могли б і взагалі нічого не писати. Тема листа повинна перегукуватись з самим текстом листа.

Якщо, відповідаючи на лист, ви міняєте тему розмови, пам’ятайте, що потрібно змінити і тему (назву) листа.

Довжина, зміст і формат листа

Довжина листа повинна відповідати стилю бесіди.

Наприклад, якщо ви просто відповідаєте на питання, намагайтеся робити це коротко і по суті. Завжди дотримуйтесь теми розмови. Якщо ви хочете поговорити на нову тему, краще надіслати окремий лист, тоді адресат зможе зберігати його окремо. Не пишіть весь текст листа великими літерами (він не є читабельним) та намагайтесь розбивати текст на логічні абзаци і уникайте надмірно довгих речень.

Пишіть грамотно, адже лист, повний помилок, дуже важко та неприємно читати. Уникайте флеймів – листів, які написані під впливом сильних емоцій, щоб потім не жалкувати про сказані слова.

Пам’ятайте про безпеку і не пересилайте в електронних листах конфіденційну інформацію (номери кредиток, рахунок в банку тощо).

Відповіді

Електронна пошта – це не особиста розмова чи розмова по телефону, тому адресат може забути про що йшлося в попередньому листі, особливо, якщо він веде активну переписку. Тому намагайтесь включати уривки попередньої розмови у вашу відповідь, а також відокремлювати ваш текст і той, що цитується спеціальними знаками (>). Але не зловживайте цитуванням попередніх листів. Коли назад ви отримуєте власний лист в повному обсязі (як коментар) з маленькою припискою в кінці «я згоден» – це не зовсім етично. Не змішуйте у листі інформацію загального та особистого характеру. Якщо ви отримали лист в результаті електронної розсилки, не варто повідомляти адресату, що ви його отримали (звісно, якщо у вас не попросять дати відповідь).

Підписи

Підпис електронного листа – це невеликий текстовий уривок в кінці повідомлення, який, зазвичай, містить контактну інформацію. Більшість мейлерів мають функцію автоматичного прикріплення підпису до вихідних листів. Це важливий елемент повідомлення, але і тут варто знати міру. Підпис повинен бути коротким, але інформативним (4-7 рядків цілком достатньо). Довгі підписи завантажують канали зв'язку. Він має ідентифікувати вас: прізвище, ім’я, посада, місце роботи (якщо ви ведете ділову переписку). Також, обов’язково вказуйте контактну інформацію: телефон, факс, скайп.

Прості правила ввічливості

Електронна пошта – це засіб зв’язку між людьми, тому без правил ввічливості тут не обійтись. Не забувайте сказати «будь-ласка», якщо ви звертаєтесь до когось з проханням, і, звісно, ніколи не завадить сказати «дякую», якщо хтось допоміг вам. Ми не забуваємо про такі моменти ввічливості в реальному житті і не варто ними нехтувати під час віртуального спілкування.

Не чекайте відповідь на ваш електронний лист негайно. Те, що вам не відповіли протягом кількох хвилин, зовсім не означає, що вас ігнорують. Зауважте, що не існує на сто відсотків надійної поштової системи, тому намагайтесь не писати в електронному листі конфіденційну інформацію (якщо ви попередньо її не зашифруєте за допомогою надійної програми для шифрування інформації). Пам’ятайте про адресата, адже ви не єдина людина, яка може постраждати у випадку, коли конфіденційне повідомлення набуде розголосу в мережі.

Намагайтесь завжди більш повно викладати інформацію по темі в електронному листі. Якщо це прохання допомоги в певному питанні, адресат повинен володіти найбільш розширеною інформацією, щоб зуміти допомогти вам.

3. Культура спілкування у форумах, чатах та соціальних мережах

На будь-якому форумі, у чаті або в соціальних мережах існують свої правила спілкування. Наприклад, спілкування в професійних, тематичних форумах, чатах та співтовариствах характеризується певним рівнем кваліфікації та знань, де потрібно бути компетентним в тих чи інших питаннях. В молодіжних форумах або ж чатах більш поширена анонімність та сленги, немає чітких рамок у висловлюваннях. Тому, перед тим як вступити в обговорення у якусь із спільнот, бажано звернути увагу на місцеві правила комунікації, щоб в подальшому мирно співіснувати з її учасниками.

Важливі правила спілкування у форумах, чатах і соціальних мережах:

• Намагайтесь бути толерантними.
• Не ігноруйте правила культурного спілкування для різних Інтернет-ресурсів.
• Пишіть коротко та зрозуміло.
• Будьте об’єктивними.
• Слідкуйте за граматикою.

Загальноприйняті правила поведінки в чатах та форумах:

• Не роздавайте поради, якщо не компетентні в якомусь питанні, і не розміщуйте свідомо помилкову інформацію.
• Не створюйте теми, які вже раніше обговорювались,та не дублюйте їх на інших форумах.
• Намагайтесь не створювати теми, назви яких не відображають саму сутність питання, наприклад: «Help», «SOS», «Допоможіть» тощо.
• Не зловживайте цитуванням повідомлень інших учасників обговорень (оверквотинг).
• Не флейміть. Тобто не відходьте від основної теми обговорення, відволікаючись на конфліктні ситуації: суперечки, образи тощо. В мережі існує правило – ніколи не відповідати на флейм. Флейми краще залишати без уваги та ігнорувати «флеймерів», а урегулювання конфліктів залишити на модераторів.
• Не офтопте. Офтопити – це означає надсилати повідомлення, які не відповідають обговорюваній темі, в тому числі обговорювати особисті питання, для цього існують Особисті Повідомлення.

Зверніть увагу на шрифт. Не пишіть суцільними заголовними літерами, або ж лише курсивом чи жирним шрифтом. Текст повинен мати читабельний вигляд. Більшість форумів видаляють повідомлення, які мають більше третини тексту в такому вигляді.

• Не зловживайте смайликами. Інколи за смайликами неможливо розібрати текст і те, що хотів донести автор, тому краще писати більше по темі і слідку-вати, де смайлик є доречним, а де ні.

• Дотримуйтесь трьох «НЕ»:

- не провокуйте скандалів;
- не переходьте на особистості;
- не пропагуйте/не заохочуйте/протизаконні дії.

• Не будьте фанатами.

•Не розміщуйте комерційну рекламу та спам, а також не хваліть на форумах компанії, програми, товар тощо, даючи посилання на них в мережі, – це розцінюється як реклама та видаляється. Дані дії можуть заохочуватись у соціальних мережах (або ж в окремих розділах форуму), коли в групі створюється тема на зразок «радимо».

• Не обговорюйте дії модератора. Краще питання модератору надсилати в Особисті Повідомлення.

• Найголовніше – залишайтесь ввічливими один до одного, адже це основне правило хорошого віртуального спілкування.

4. Мережевий сленг

У сучасному Інтернет - просторі існує власний комп’ютерний сленг – це так звана «мова», яка виникла з появою перших електронно-обчислювальних машин (ЕОМ). Спочатку нею спілкувались професіонали в комп’ютерній сфері, але сьогодні його використовують майже всі користувачі Інтернету. Комп’ютерна лексика містить багато слів та скорочень англійської мови. Це тому, що Інтернет має американське коріння і довгий час мовою мережі залишалась саме англійська мова.

Мережевий сленг складається із слів перероблених або ж навмисно перекручених чи скорочених. Наприклад, «юзер» (користувач) бере початок від англійського user, а «шутер» (гра-15стрілялка) від англійського shoot– стріляти.

Нових значень в даному слензі набули і українські дієслова, наприклад, «приблуда» – програма, що працює разом з якою-небудь іншою програмою; лексема «деза» походить від скороченого «дезінформація»; «перекачати», «злити» – переписати інформацію тощо.

Досить популярними в мережевому слензі є скорочені слова. Найчастіше їх використовують з метою написання повідомлень за рекордно короткий час, або коли часу на відправку повідомлення обмаль. В деякій мірі це також викликано прагненням втаємничити свою розмову від тих, хто має можливість її побачити. Наприклад, в нову версію Великого Оксфордського

словника було внесено найпоширеніші вислови з мережевого сленгу – OMG(«Oh my God») і LOL(«laughing out loud» –сміятися вголос), а також символ <3, що нагадує серце і замінює в листуванні дієслово «любити». Ще раніше у Великий Оксфордський словник уже були включені скорочення IMHO («in my humble opinion» – на мою скромну думку), TMI («too much information» – дослівно – надто багато інформації або, як часто пишуть у рунеті, «многабукаф») і BFF («best friends forever» – кращі друзі навіки»).

Крім того, в мережі активно використовуються цифри і окремі літери, які при усному мовленні звучать так само, як окремі слова або частини слів. Наприклад, «4u» – означає «For You»(для тебе), «2 nite» – це скорочена і кілька спотворене «tonight» (сьогодні ввечері). Майже всі скорочення походять від англійської мови, тому, використовуючи такі скорочення, потрібно зауважити, що не всі адресати ваших повідомлень можуть їх розшифрувати.

Сьогодні в українському Інтернет - просторі з’являється альтернатива англійським скороченням.Наприклад,українські інтернетівці часто використовують скорочення НМД (На Мою Думку) замість IMHO(In My Humble Opinion – На мою скромну думку); НМВ (Наскільки мені відомо) замість AFAIK (As Far As I Know – Наскільки мені відомо); ЗУСМ (Зараз умру зо сміху) замість LOL (Laughing Out Loud –Сміятися вголос); ОП (Особисті повідомлення) тощо.(Додаток 1;2)

IV
Інформація для педагогів

Питання безпечного перебування дитини в Інтернеті повинно вирішуватися, насамперед, педагогами: саме їх діяльність покликана виробляти потрібні компетенції з кібербезпеки не лише у дітей, а й у їх батьків, адже навчання будь-якому захисту - це неперервний процес, який не закінчується межами закладу освіти.

Тому пропонуємо наступний алгоритм «спілкування» з Інтернетом:

І. Виконуйте три основні правила:

1.Приділяйте увагу захисту устаткування та інформації:

- регулярно оновлюйте операційну систему;
- використовуйте антивірусну програму;
- застосовуйте брандмауер;
- створюйте резервні копії важливих файлів;
- будьте обережні при завантаженні нових файлів.

2. Захистіть себе в онлайн:

- з обережністю розголошуйте особисту інформацію;
- думайте про те, з ким про що розмовляєте;
- пам’ятайте, що в Інтернеті не вся інформація надійна та не всі користувачі відверті.

3. Дотримуйтеся правового поля:

- законів потрібно дотримуватися навіть в Інтернеті;
- дотримуйтеся загальноприйнятих норм спілкування;
- при роботі в Інтернеті не забувайте піклуватися про інших так само, як про себе.

ІІ. Створіть безпечну зону та контролюйте дотримання дитиною меж цієї зони.

Спробуйте разом з дитиною знайти корисні, цікаві й безпечні сайти, які вона переважно буде відвідувати надалі. Періодично відвідуйте їх разом. З таких сайтів сформуйте список дозволених сайтів в програмному забезпеченні системи мережної безпеки вашої системи, наприклад - для цього можна застосувати налаштування параметрів оглядача (не забудьте при цьому програмно заборонити доступ до налаштувань зі сторони інших користувачів). В цьому випадку, якщо дитині необхідно зайти на новий сайт, їй доведеться попросити вашої допомоги на додавання його адреси в перелік дозволених сайтів, отже ви матимете змогу оцінити безпечність сайту до того, як він стане вільно доступним дитині. Крім того, корисно встановити програму-фільтр. За допомогою програм фільтрації можна встановити обмеження веб - сайтів на основі змісту. Це означає, що встановивши і настроївши таку програму, ви можете заблокувати для дитини доступ до сайтів, які містять матеріали, визначені як небезпечні (порнографія, насильство, суїцид тощо).

ІІІ. Опрацюйте зазначені матеріали.

З метою надання допомоги з питань захисту дітей від впливу шкідливої інформації розроблено ряд посібників і складено перелік рекомендованих для дітей онлайн - ресурсів, які допоможуть відкрити дітям цікавий, корисний і, головне, безпечний Інтернет.

Міністерство освіти і науки пропонує використовувати батькам (і педагогам) такі основні джерела:

1. 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).

2. 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).

3. Безпечне користування сучасними інформаційно-комунікативними технологіями / О. Удалова, О. Швед, О. Кузнєцова [та ін.]. – К.: Україна, 2010. – 72 с.

4. Памятка для батьків «Діти. Інтернет. Мобільний зв’язок», розроблена Національною експертною комісією України з питань захисту суспільної моралі (http://www.moral.gov.ua/news/311/).

5. Перелік рекомендованих для дітей онлайн - ресурсів, затверджений на засіданні Національної експертної комісії України з питань захисту суспільної моралі (рішення від 20.04.2010 № 2).

Список використаної літератури

1 Безпечне користування сучасними інформаційно-комунікативними технологіями / О. Удалова, О. Швед, О. Кузнєцова [та ін.]. – К.: Україна, 2010. – 72 с.

2. Білинська Є., Жичкина А. Сучасні дослідження віртуальної комунікації: проблеми, гіпотези, результати. - М.: ЮНИТИ - ДАНА, 2004. - 165 з.

3. Виховання культури користувача Інтернету. Безпека у всесвітній мережі: навчально-методичний посібник / А. Кочарян, Н. Гущина. – К., 2011. – 100 с. (http://www.mon.gov.ua/newstmp/2011/18_02/3/4press.pdf).

4. Віртуальна «реальність» публічних бібліотек: метод. поради / упоряд. О. Шматько, С. Дмитрів. –Л. Ліга-прес, 2011 . –40 с. (Секрети бібліотечної майстерності).

5.Горявский Ю. Назад у майбутнє // Світ Internet. №10. - М., 2001. - 35 з.

6. 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).

7. Додаток: Комп'ютерний сленг [Електронний ресурс]: сайт Вікісловник: Вільний словник . –Режимдоступу: http://bit.ly/1wQ1IS8. – Назва з екрану.

8. Етика спілкування. Проблеми віртуальної реальності[Електронний ресурс]: сайт Етика сьогодні: Акту-ально про етику та мораль . – Режим доступу: http://www.etica.in.ua/etika-spilkuvannya-problemi -virtual-noyi-real-nosti/. – Назва з екрану.

9. Жичкина А. Соціально-психологічні аспекти спілкування з Інтернету. - М.: Дашков і Ко, 2004. - 117 з.

10. Інтернет - діалект [Електронний ресурс]: сайт Тиждень. ua
–Режим доступу: http://tyzhden.ua/Publication/2520. – Назва з екрану.

11. Інтернет-скорочення [Електронний ресурс]: сайт Computer.lviv.ua.–
Режим доступу: http://computer.lviv.ua/docs/internet-sleng. –Назва з екрану.

12. Культура віртуального спілкування: навчально-методичний посібник - Х., 2014.

13. Культура віртуального спілкування: метод.- бібліогр. матеріали / уклад. Є. Кулик, О. Бартош: ред. В.Кучерява, С. Чачко; ДЗ Державна б-ка України для юнацтва. –К., 2010. –65 с.

14. Мережевний етикет [Електроресурс]: сайт Етикет від А до Я .–Режим доступу :http://www.etiket.ru/contact/email.html. – Назва з екрану.

15. Мережевний етикет [Електроресурс]: сайт KONTAKTE.SU: Блоги та соціальна мережа. Дискусійні форуми . – Режим доступу:
http://kontakte.su/setevoy-etiket. –Назва з екрану.

16. Мережевий сленг офіційно увійшов в англійську [Електронний ресурс]: сайт Укрінформ. –Режим доступу: http://bit.ly/Uk80wZ. –Назва з екрану.

17. Мережевий сленг поповнив Оксфордський словник англійської мови [Електронний ресурс]: сайтDW. –Режим доступу:http://bit.ly/1nZ8aFM. – Назва з екрану.

18. Микосовський М. Моральний кодекс інтернетівця (нетикет) Електронний ресурс]: сайт Дивен світ. – Режим доступу: http://dyvensvit.org/blogs/467.html. –Назва з екрану.

19. Мистецтво спілкування в Інтернеті, чи казкотерапія діє // Світ ПК. - 2003. - 215 з.

20. Нетикет та культура віртуального спілкування: метод. поради / упорядник О. Шматько, О. Дудок; ЛОУНБ. –Л. : Ліга-Прес, 2013 . –44 с.

21. Пам’ятка для батьків "Діти. Інтернет. Мобільний зв’язок”, розроблена Національною експертною комісією України з питань захисту суспільної моралі (http://www.moral.gov.ua/news/311/).

22. Петрова Н.П. Комп'ютерна освіта: несприятливий прогноз? - 2006. - N7.

23. Петров Д. Мобільна революція // Світ Internet. – 2001.

24. Словник термінів [Електронний ресурс]:сайт Веб-спілкування, нетикет .–Режим доступу: http://netiquette4uth.blogspot.com/p/blog -page.html.– Назва з екрана

Додаток 1

Словник термінів

Аватар (аватарка)–зображення, обличчя користувача у віртуальному просторі.

Бан–один з прийнятих в Інтернеті способів контролю за діями користувачів. Як правило, бан полягає в обмеженні певних прав користувача (на створення/відправлення нових повідомлень або створення нових тем на веб-форумі, на відправлення повідомлень в чаті, на коментування в блогах та ін.) в цілях захистити інтернет-сайт від тролів, спамерів, вандалів та інших осіб, чиї повідомлення шкодять продуктивній роботі ресурсу.

Блогер – автор блогу.

Веб 2.0–зведена назва для сукупності нових технологій, методів та підходів до побудови інформаційних відносин в Інтернеті.

Веб-серфінг – «подорож» Інтернетом.

Геймер – людина, що грає в комп'ютерні ігри.

Гіпертекст (англ. hypertext) –текст для перегляду на комп'ютері, що містить зв'язки з іншими документами (гіперзв'язки, гіперпосилання); користувач може перейти до пов'язаних документів з вихідного (первинного) тексту попередньо активізувавши посилання.

Гість–відвідувач форуму, який може продивлятись теми та повідомлення форуму, але без права їх публікувати.

Живий журнал(Livejournal.com) –один з наймасштабніших блог-сервісів.

Електронна пошта (e-mail) – Інтернет-сервіс для обміну даними будь-якого змісту (текстові документи, аудіо-відеофайли, архіви, програми).

Емограма–графічний символ, що використовується для вираження емоцій.

Капс, капостити (Caps Lock)–це написання деякими користувачами мережі Інтернет повідомлень заголовними 19літерами, що не вітається на багатьох форумах, чатах та забороняється, так як розцінюється, як крик та підвищення тону (тільки у виняткових випадках можна використовувати, щоб привернути увагу, наприклад, попрощатися).

Контент(англ. content–зміст) –наповнення будь-якого інформаційного ресурсу (веб-сайту, блогу тощо) –тексти, графіка, мультимедіа.

Кросспостинг–розміщення однакових за змістом пові-домлень/тем в різних розділах/темах форуму або в одному і тому ж розділі/темі форуму з метою залучення уваги до власної персони.

Модератор(англ. moderator)–людина, що відповідає за дотримання встановлених норм поводження у Інтернет-ресурсах, частіше форумах.

Некропост(від грец. νεκρός –мертвий і англ. post над-силати, повідомлення) – повідомлення на форумі, написане в давно забутій темі, в результаті чого вона піднімається на першу сторінку.

Нетизянин, нетизяни(англ.netizen) –активний корис-тувач Інтернету.

Нетикет(неологізм, що є злиттям слів «мережа» [англ. net] і «етикет») – правила поведінки, спілкування в Інтернеті.

Нік – (англ. nick, nickname–прізвисько) –переважно вигадане ім'я, яким називає себе користувач Інтернету на різно -манітних чатах, форумах, месенджерах тощо.

Оверквотинг – надмірне цитування.

Офтопік – повідомлення, що не відповідає темі поточного обговорення.

«Под катом» – блог-вислів, що означає перенесення продовження публікації на другу сторінук. Як правило, великі публікації в блозі ділять на дві частини –анотація і повний текст публікації.

Пост – окреме повідомлення на форумі.

Прев'юшки – це невелика картинка, натиснувши на яку відкривається картинка оригінального розміру.

Провайдер (англ. provide–надавати) – компанія, що надає послуги доступу до Інтернету.

Сервер (англ. server) – програмне забезпечення, що приймає запити від комп'ютерів-користувачів.

Сервер (англ. server) – комп'ютер (чи спеціальне комп'ютерне обладнання), призначене для виконання певних сервісних функцій.

Сленг – діалект, жаргон, набір фраз та висловів, що мають вузьке застосування та не є граматично правильними словами в мові.

Смайлик (англ. smile–посмішка) – зображення, складене з розділових знаків, букв і цифр, що використовується для передачі емоцій користувача під час спілкування в Інтернеті.

Спам – небажані поштові повідомлення, зазвичай рекламного характеру, що надходять від невідомих людей та організацій без згоди одержувача.

Тред – (англ. thread–нитка)на форумах, в блогах, списках розсилки, конференціях – послідовність відповідей на повідомлення, тобто «гілка обговорень».

Тролінг (англ.trolling) – розміщення в Інтернеті провокаційних повідомлень з метою викликати конфлікти між учасниками, образи, війну правок, марнослів'я тощо. Особу, яка займається тролінгом, називають тролем.

Флейм–процес, що виникає в Інтернеті, своєрідна «словесна війна».

Флуд – повідомлення у форумах і чатах, що займають Великі об’єми і не несуть корисної інформації.

Френд-стрічка – сторінка, на якій відображаються всі повідомлення певного користувача Живого Журналу. Аналогічні френд-стрічки є в більшості соціальних мереж.

Хакер – особа, яка зламує інформаційну мережу чи систему організації, або використовує її, не маючи на це дозволу. Термін «хакер» має також інше значення –так іноді називають досвідчених комп’ютерних користувачів.

Хостинг – послуга з надання дискового простору для фізичного розміщення інформації на сервері, що постійно знаходиться в Інтернеті.

Чат – засіб для спілкування користувачів Інтернету в режимі реального часу, в якому користувачі можуть писати повідомлення, що миттєво, одне за одним, відображаються на екрані.

ICQ – абревіатура, складена на основі аудиального звучання назви програми для спілкування он-лайн «Iseek you », «Я шукаю тебе». ICQ забезпечує миттєве відправлення та отримання текстових повідомлень.

Додаток 2

Інтернет - скорочення

10X (Thanks)–Дякую.
2DAY (Today)–Сьогодні.
2MORO (Tomorrow)–Завтра.
4 (For) –Для.
4GET (Forget)–Забудь.
ADDY (Address) –Адреса.
AFAIK (As Far As I Know) –Наскільки мені відомо.
AFTK (Away from the keyboard)–Мене нема за клавіатурою.
ANY1 (Any one) –Кожен.
ASAP (As Soon As Possible) –Якомога швидше.
ASL (Age/sex/location) –Вік, стать, місце перебування.
ATM (At the moment) –В дану хвилину, зараз.
B4 (Before)–Раніше.
BBIAF (Be back in a few minutes) –Повернусь за кілька хвилин.
BBIAH (Be back in an hour) –Повернусь за годину.
BBIAM (Be back in a minute) –Повернусь за хвилину.
BBIAS (Be back in a second) –Повернусь за секунду.
BBL (I'll be back later)–Повернусь пізніше.
BBS (Be back soon) –Скоро повернусь.
BE4 (Before) –Перед.
BF (Boyfriend)–Хлопець.
BRB (Be Right Back) –Скоро повернусь.
BTW (By The Way) –До речі.
C (See)–Бачу.
CU (See You) –Побачимось.
CYA (See You)–Побачимось.

DETAI (Don't Even Think About It) –Навіть і не думай про це.
EM (Them) –Вони.
F2F (Face to face) –Тет а тет, віч-на-віч.
FAQ (Frequently asked questions) –Часто задавані питання.
FU (Fuck up) –Безлад.
FW (Freeware) –Безкоштовно.
FYI (For your information)–До вашого відома.
GF (Girlfriend) –Дівчина.
GR8 (Great) –Прекрасно!
GTG (I got to go) –Мені треба йти.
H8 (Hate) –Ненавиджу.
HAND (Have A Nice Day) –Гарного дня!
HP (Homepage)–Домівка.
HTH (Hope this help)–Сподіваюсь, це допоможе.
IC (I see) –Зрозуміло.
IDK (I Don't Know) –Я не знаю.
ILUVU (I Love You)–Я тебе люблю.
IMHO (In My Humble Opinion)–На мою скромну думку.
IMO (In my opinion) –На мою думку.
IOW (In other words) –Іншими словами.
IRL (In the real life) –В справжньому житті.
JK (Just kidding) –Просто жарт.
K (Ok)–Окей.
KIT (Keep In Touch) –Залишайся на зв’язку.
L8 (Late) –Пізно.
L8R (Later)–Пізніше.
LOL(Lot of laugh, laughing out laud)–Купа сміху.
M8 (Mate)–Друг.
ME2 (Me too)–Я теж.
MSG (Message) –Повідомлення.
NO1 (No one) –Ніхто.
NP (No problems) –Без проблем.
OIC (Oh, I see) –Зрозуміло.
PCM (Please Call Me)–Будь-ласка,подзвони мені.
PLS(Please)–Будь-ласка.
POV (Point of view) –Точка зору.
PPL (People) –Люди.
RE (How are you) –Як справи?
RL (Real life) –Справжнє життя.
ROFL (Rolling on the floor laughing) –Котитись по підлозі від сміху.
RUOK (Are You OK) –З тобою все гаразд?
SMT (Something) –Щось.
SUP (What's up) –Як справи.
TFHAOT (Thank for help ahead of time)– Наперед вдячний.
THX/THS (Thanks) –Дякую.
U (You) –Ти.
U2 (You too) –Ти теж.
W8 (Wait) –Зажди.
WB (Welcome back) –З поверненням.
WBR (With best regards) –З найкращими побажаннями.
WKND (Weekend) – Вихідні.
WRT (With respect to)– З повагою.