

Інститут інноваційних технологій і змісту освіти
Міністерства освіти і науки, молоді та спорту

Компанія «Майкрософт Україна»

Кочарян А.Б., Гуцина Н.І.

Виховання культури користувача Інтернету. Безпека у всесвітній мережі

Навчально-методичний посібник

Київ – 2011

Рекомендовано Міністерством освіти і науки, молоді та спорту
для використання у навчально-виховному процесі

(лист від 27.12.10 р. № 1/11-12128)

**«Виховання культури користувача Інтернету. Безпека у
всесвітній мережі»:** навчально-методичний посібник /

А.Б. Кочарян, Н.І. Гуцина. - Київ, 2011. – 100 с.

У навчально-методичному посібнику містяться загальні методичні рекомендації для вчителів, а також батьків, з формування у дітей компетентцій грамотного та безпечного використання Інтернет-ресурсів.

Рецензенти:

В.М. Оржеховська, д-р пед. наук, професор, завідувачка лабораторії превентивного виховання Інституту проблем виховання НАПН України;

Н.А. Саражинська, вчитель інформатики спеціалізованої загальноосвітньої школи I-III ступенів №12 з поглибленим вивченням інформаційних технологій м. Білої Церкви

Упорядники: Я.А.Курченко, А.Б.Кочарян

Відповідальна за випуск *Пушкарьова Т.О.*

Редактор *Бігун Н.М.*

Комп'ютерна верстка *Громська О. І.*

Видання здійснено за підтримки програми Microsoft

«Партнерство в навчанні»

© Інститут інноваційних технологій і змісту освіти
Міністерства освіти і науки, молоді та спорту

© Компанія «Майкрософт Україна»

Шановні колеги!

Якщо ви використовуєте інформаційно-комунікаційні технології у навчально-виховному процесі загальноосвітніх навчальних закладів, то цей посібник, безперечно, буде для вас корисним. Ми намагалися створити саме таку книжку, яка б допомогла вам підготувати дітей та молодь до свідомого, грамотного, а головне - безпечного використання інформаційних ресурсів, виховати культурних користувачів мережі Інтернет.

У I розділі посібника йдеться про роль інформаційно-комунікаційних технологій у сучасному навчальному закладі, аналізуються зміни, які відбуваються у навчально-виховному процесі завдяки використанню інформаційних інновацій.

У II розділі наводяться дані статистичних досліджень щодо використання ресурсів мережі Інтернет дітьми та молоддю України, розповідається про можливості, які відкриваються для розвитку молодого покоління завдяки всесвітній мережі, а також подається систематизований список Інтернет-загроз для дітей.

III розділ спрямований на формування у дітей компетенцій грамотного та безпечного використання Інтернет-ресурсів, виховання культури поведінки у мережі Інтернет. У цьому розділі пропонуються загальні методичні рекомендації для вчителів з формування у дітей зазначених компетенцій та подаються структурно-логічні моделі:

- підготовки педагогів-тренерів з безпеки в Інтернеті,
 - організації навчально-виховної роботи з дітьми 7-10 років,
 - організації навчально-виховної роботи з дітьми 11-18 років
- та
- алгоритми проведення цих робіт.

Структурно-логічні моделі було створено та апробовано в рамках програми «Онляндія – безпечна Web-країна». Ми

намагалися узагальнити великий практичний досвід тренінгової діяльності волонтерів цієї першої в Україні освітньої програми з безпеки дітей в Інтернеті.

У IV розділі пропонуються методичні рекомендації для превентивної роботи з батьками та структурно-логічна модель тренінгу для батьків з безпеки в Інтернеті.

У додатку подаються матеріали, які допоможуть в організації та проведенні тренінгів: вправи на знайомство, на формування мотивації до діяльності тощо; питання, які найчастіше виникають під час проведення тренінгу, та відповіді на них, додаткова цікава інформація, коментарі тощо.

Окремим блоком у додатку розміщено матеріал, який можна використати для роботи з батьками: при підготовці батьківських зборів, інформаційних повідомлень, роздруківок, бесід тощо.

У посібнику використано матеріали Інтернет-ресурсів з безпеки дітей в Інтернеті, досвід педагогів і тренерів України, які працюють у цій тематиці, та власний практичний тренінговий досвід.

Практичні матеріали, які пропонуються у цьому посібнику, можуть бути використані на уроках з інформатики, основ здоров'я, правознавства, з курсу «Людина і світ» та у позакласній роботі: під час проведення виховних годин, літньої практики - та у роботі з батьками, зокрема під час проведення батьківських зборів.

Зі щирими побажаннями успіхів у роботі

Автори

РОЗДІЛ І. ІНФОРМАЦІЙНО-КОМУНІКАЦІЙНІ ТЕХНОЛОГІЇ У СУЧАСНОМУ НАВЧАЛЬНОМУ ЗАКЛАДІ

Інформаційно-комунікаційні технології або ІКТ — технології, пов'язані зі створенням, збереженням, передачею, обробкою та управлінням інформацією. Цей широко вживаний термін включає в себе всі технології, що використовуються для спілкування та роботи з інформаційними ресурсами.

Концепція *інформаційних технологій* виникла у 1980-ті роки і була віднесена до елементу *комунікації*. Наразі інформаційно-комунікаційні технології включають апаратні засоби (комп'ютери, сервери тощо) та програмне забезпечення (операційні системи, мережеві протоколи, пошукові системи тощо).

У свій час Цицерон сказав: «Не настільки прекрасно знати латину, як ганебно її не знати». Сьогодні це стосується інформаційно-комунікаційних технологій. У сучасному світі ІКТ є важливою і невід'ємною частиною держави, бізнесу та приватного життя. Тому впровадження ІКТ – один із пріоритетних напрямків сучасної освіти. Головною метою її розвитку є забезпечення загального доступу до освітніх ресурсів шляхом інтенсивного впровадження новітніх методів навчання, комп'ютеризації та інформатизації. Комп'ютери мають перейти із кабінету інформатики у навчальні класи, призначені для вивчення фізики та географії, літератури та музики, хімії та біології...

Раніше інформацію з будь-якого предмета чи теми учень міг отримати з підручника, довідкової літератури, лекції вчителя, конспекту уроку. Сьогодні, з огляду на сучасні реалії, вчитель повинен використовувати нові методи роботи, спираючись на ІКТ. Це обумовлено тим, що в наш час кожні 72 години кількість інформації збільшується вдвоє, тому потрібні спеціальні навички, вміння та сучасні засоби для опрацювання такого величезного інформаційного об'єму. До того ж, сучасні діти народилися у цифровому світі XXI століття, тому з раннього віку знайомі з мобільними телефонами, ноутбуками, плеєрами. Потужний потік нової інформації, реклами, застосування комп'ютерних технологій на телебаченні, розповсюдження ігрових пристроїв, електронних іграшок і комп'ютерів впливають на виховання дитини та сприйняття нею навколишнього світу. Істотно змінюється і характер її найпершої практичної діяльності - гри, змінюються й улюблені герої та

захоплення. Тому дитина легко сприймає на уроці інформацію, подану за допомогою медіа-засобів, оскільки вони є звичними, природними для неї.

Традиційна класно-урочна система зорієнтована на трансляцію знання від учителя до учня. Використання ІКТ у навчально-виховному процесі дозволяє перейти від навчання, в основі якого - інформація, почута з вуст викладача або прочитана в підручнику, до навчання через сприймання інформації з електронних ресурсів, Інтернету, навколишнього середовища тощо. На будь-якому уроці вчитель, оперуючи різноманітними цифровими навчальними ресурсами, може організувати дослідницьку діяльність учнів, зорієнтувати в індивідуальній роботі на поглиблений пошук інформації, навчити оцінювати надійність різних інформаційних джерел, створювати власні електронні продукти: малюнки, мультимедійні презентації, електронні моделі. Втрачає сенс необхідність переважувати пам'ять дитини великим об'ємом знань. Набагато важливіше навчити дитину знаходити їх і користуватися ними на практиці, застосовувати в життєвих реаліях. Крім того, можливості, що відкриваються завдяки використанню ІКТ, дозволяють дітям навчатися в індивідуальному темпі, забезпечують ситуацію успіху для кожного учня, допомагають зробити процес здобуття знань захоплюючим і створюють міцну мотивацію до навчання.

Комп'ютерні технології відкривають і для вчителя нові можливості, дозволяючи разом з учнем отримувати задоволення від процесу пізнання світу, зануритися в яскравий, барвистий світ нових знань.

Поєднання традиційних методів навчання та сучасних інформаційних технологій дозволяє зробити процес навчання мобільним, строго диференційованим та індивідуальним.

Отже, перевагами використання ІКТ є:

- індивідуалізація навчання;
- інтенсифікація самостійної роботи учнів;
- збільшення обсягу виконаних на уроці завдань;
- підвищення мотивації та пізнавальної активності за рахунок різноманітних форм роботи, завдяки можливості включення ігрового моменту (наприклад: розв'яжеш приклади - відкриєш картинку, вставиш правильно всі букви - наблизити до мети казкового героя);
- розширення інформаційних потоків та обсягу нових знань завдяки використанню **мережі Інтернет**.

РОЗДІЛ II. ІНТЕРНЕТ В УКРАЇНІ

В Україні кількість користувачів Інтернету щороку стрімко зростає. Так, згідно з показниками сайту Sputnikmedia.net [18], у січні 2006 року українська Інтернет-аудиторія складалася з 4 207 391 особи.

Станом на 1 січня 2007 року, за повідомленням прес-служби департаменту зв'язку та інформатизації Міністерства транспорту та зв'язку, в Україні налічувалося вже біля 9 млн. користувачів, а це - 18,75% від кількості жителів України.

Кількість користувачів українського Інтернету в травні 2008 року зросла на 0,77% порівняно з квітнем і складала 8 471 954 осіб на місяць; станом на березень 2009 року - 11,96 млн. осіб, що на 9,4% більше, ніж у лютому 2009 року [19].

У квітні 2010 року дослідження «Gemius Україна» виявило 8,669 млн. регулярних користувачів Інтернету віком від 16 років і старших. У той самий час на замовлення ІнаУ були опубліковані дані «InMind»: 12 млн. користувачів Інтернету в Україні.

У червні 2010 року «Бігмір Інтернет» нарахував уже 18 581 501 унікальних користувачів [19].

Отже, якщо порівняти кількість користувачів Інтернету в січні 2006 року (4 207 391 особа) та у червні 2010 року (18 581 501 особа) висновок можна зробити один: з кожним роком кількість українців, які використовують ресурси всесвітньої мережі Інтернет, збільшується (див. діаграму1).

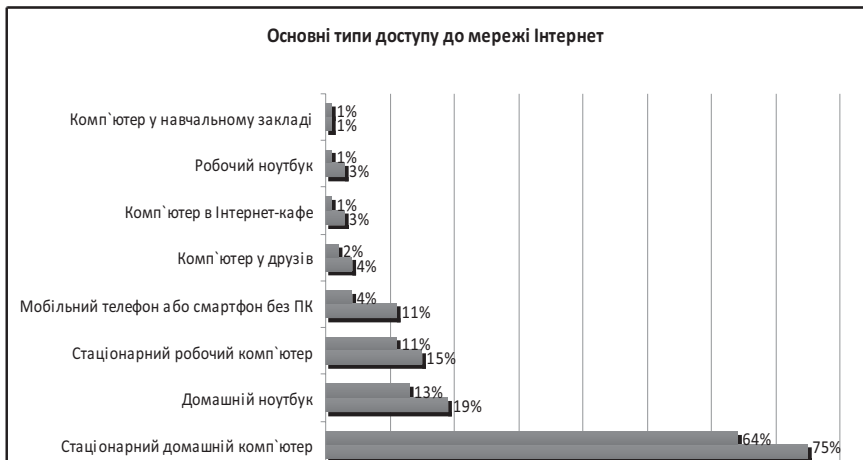
Діаграма 1



Лідерами за кількістю нових користувачів стали соціальні мережі. Тепер 31% користувачів Інтернету в Україні відвідують ці ресурси. Також великою популярністю користуються сайти новин (кількість відвідувачів у віковій групі від 30 до 49 років зросла тут з 24% до 29%) і сайти з мультимедійним контентом (з 26% до 32% збільшилася кількість користувачів, які завантажують музику і фільми, і з 9 % до 14% зросла кількість тих, хто переглядає он-лайн-відео або слухає он-лайн-радіостанції).

Основні типи доступу до мережі Інтернет українських користувачів [4] відображені на діаграмі 2.

Діаграма 2



1. Діти в Інтернеті. Дослідження з проблем використання Інтернету дітьми в Україні

Як свідчать результати дослідження Eurobarometer [5], проведеного у 2008 році у 27 країнах - членах ЄС, 75 відсотків дітей віком від шести до 17 років активно користуються Інтернетом. Причому це стосується також половини дітей тих батьків, котрі самі у всесвітню мережу - ні ногою! «Техніку он-лайн-безпеки» батьки обговорювали

лише з кожним другим малолітнім «мережевиком». У 92 відсотках випадків мова йшла про неприпустимість розголошення особистої інформації, у 83 відсотках — про небажаність спілкування з незнайомими людьми. 59 відсотків батьків, щоб убезпечити дітей від негативних інформаційних впливів, використовують спеціальні фільтри або моніторингове програмне забезпечення. 64 відсотки батьків, які цього не роблять, стверджують, що довіряють своїм дітям. 14 відсотків зізналися, що просто не знають, як ці програми встановлюються.

Інше дослідження, яке було проведено в 2009 році в рамках проекту EU Kids Online [6] в Лондонському економічному інституті (London School of Economics), висвітило зовсім інші результати. Згідно з цим дослідженням, у Великій Британії 77% родин використовують спеціальні програми, які фільтрують зміст Web-сторінок. 87% батьків проводять бесіди з дітьми щодо безпечного користування Інтернетом. Але одночасно дослідники констатують факт, що британські батьки не дуже занепокоєні переглядом дорослого контенту в мережі Інтернет дітьми.

В Україні подібні дослідження розпочалися лише з 2009 року завдяки діяльності членів Коаліції за безпеку дітей в Інтернеті. Коаліція створена у 2008 році з ініціативи компанії «Майкрософт Україна».

Дослідження проводилося Інститутом соціології НАН України за підтримки компанії «Київстар», яка є членом Коаліції за безпеку дітей в Інтернеті, в період із серпня по вересень 2009 року в 11 містах України та полягало в опитуванні 1200 респондентів (дітей та дорослих) щодо якісного та кількісного використання дітьми Інтернет-ресурсів. Отримані показники насторожують: переважна більшість вчителів, дітей і їхніх батьків не поінформовані про потенційні ризики для дітей в Інтернеті та про те, як їх уникнути.

22% дітей періодично потрапляють на сайти для дорослих. 28% дітей, побачивши в Інтернеті рекламу алкоголю або тютюну, хоч раз спробували їх купити, а 11% — намагалися купити наркотики.

Понад 28% опитаних дітей готові переслати через Інтернет свої фотографії незнайомцю. 17% без коливань погоджуються повідомити інформацію про себе та свою родину: місце проживання, професію, графік роботи батьків. Для чого незнайомим людям може знадобитися така інформація, діти, як правило, не замислюються.

Близько 14% опитаних час від часу відправляють платні SMS за бонуси в он-лайн-іграх, і лише дехто з них звертає увагу на вартість такої опції.

При цьому 87% батьків вважають, що саме вони повинні навчати дітей правилам безпечного користування Інтернетом. Проте лише у 18% випадків дорослі перевіряють, які сайти відвідувала дитина.

Проведене дослідження показало, що в більшості випадків діти набагато краще від батьків обізнані з можливостями використання і мобільного, і стаціонарного Інтернету. Існує суттєва різниця між тим, як діти насправді користуються Інтернетом, і тим, що про це відомо їхнім батькам: діти користуються ним частіше, аніж думають батьки, відвідують Інтернет-кафе, сайти для дорослих, грають в азартні ігри, витрачаючи реальні гроші; контактують з незнайомцями. Про все це в більшості випадків ані батьки, ані вчителі не знають, що свідчить про високий ступінь небезпеки для дітей. Нерідко користування Інтернетом вигідне і батькам, і вчителям. Батьки часто сприймають комп'ютер та Інтернет як «кібер-няню», яка утримує дитину вдома, або як механізм, що позитивно впливає на поведінку дитини. А вчителям приносить задоволення, що діти готуються до уроків з допомогою Інтернету.

2. Інтернет-можливості для розвитку дітей

Діти, як і дорослі, використовують Інтернет з різною метою: щоб поспілкуватися з друзями, пограти в ігри, послухати та (або) записати музику, відео, підготуватися до уроків, знайти та прочитати цікаву інформацію або придбати певні товари. Для цього вони використовують наступні послуги Інтернету.

Web-браузери. Це програми, які дозволяють отримати доступ до інформації, завантаженої на інший комп'ютер. До більшості Web-сайтів доступ безкоштовний. Але окремі з них можуть запросити реєстрацію: тобто вимагати ім'я користувача, адресу електронної пошти, поштову адресу та вік. Найбільш популярним серед Web-браузерів є Microsoft Internet Explorer.

Web-сайти. Це набір Web-сторінок, об'єднаних спільною адресою, темою, логічною структурою та оформленням. Для відвідування Web-сайту необхідно знати його адресу. Наприклад, <http://www.onlandia.org.ua>

Пошукові системи. В Інтернеті існують мільйони сайтів. Саме за допомогою пошукових систем ми маємо можливість знаходити необхідну нам інформацію - проводити навігацію. Прикладом пошукової системи є <http://www.bing.com>

Електронна пошта. Це комп'ютерна версія звичайної пошти. Кожен лист має унікальну адресу, яка ідентифікує власника. Наприклад, artur.kocharyan@onlandia.org.ua. artur.kocharyan – ім'я власника електронної скриньки, а onlandia.org.ua – ім'я домену (місце, де розташована поштова скринька).

ІМ - миттєвий обмін повідомленнями. ІМ нагадує Інтернет-версію SMS. Ці програми дозволяють писати листи в режимі реального часу одночасно декільком людям, які підключилися до мережі Інтернет. Географія їхнього місцезнаходження не має значення.

IRC - Інтернет-чати. Дозволяють об'єднуватися у групи за інтересами та спілкуватися в режимі реального часу. Спілкування у чаті дуже швидке. Учасники можуть надсилати повідомлення в загальному каналі («кімнаті») одразу сотням користувачів. Загальні канали є доступними для всіх. Приватні канали («кімнати») можуть мати пароль.

Дошки оголошень. Дають можливість розміщувати невелике повідомлення або оголошення на тематичних сайтах або групах. На відміну від чатів, повідомлення може бути прочитане і в режимі офлайн: можуть пройти години, дні, доки хтось прочитає та відповідь на оголошення. Діти мають тенденцію розміщувати оголошення на дошках, які їм цікаві.

Голосові чати. Майже всі комп'ютери мають звукову карту і мікрофон для запису голосового повідомлення та можуть відправити це повідомлення іншій людині через Інтернет. Ця технологія має назву «голосовий чат».

Відеоконференції. Миттєвий обмін аудіо- та відеоматеріалами через комп'ютери.

Соціальні мережі. Це окремі Web-сайти, які дозволяють створювати власні сторінки, спільноти, розміщувати фото, аудіо- та відеоматеріали, обмінюватися миттєвими повідомленнями та слідкувати за оновленнями на сторінках друзів. Соціальні мережі досить швидко стали популярними у молоді, бо відкривають нові можливості для самореалізації та вільного спілкування.

У віртуальному просторі діти та підлітки прагнуть дізнатися щось цікаве і корисне, розслабитися та абстрагуватися від власних психологічних проблем. Інтернет для молоді – можливість цікаво та змістовно провести час.

Віртуальний світ дозволяє дітям реалізувати цілу низку базових потреб: спілкування, ігри, розваги, саморозвиток та самореалізація, виховання сміливості, вміння подолати перешкоди.

Отже, діти та підлітки в Інтернеті **спілкуються, навчаються, розвиваються та розважаються.**

3. Інтернет-загрози для дітей

Інтернет – дуже потужний ресурс, який значно полегшує життя людини та відкриває майже необмежені можливості для самореалізації та саморозвитку юної особистості, спілкування, навчання, дозвілля. Але разом з тим, в Інтернеті приховано досить багато небезпек як для дітей, так і для дорослих. Знання цих небезпек дозволить їх уникнути.

Віруси

Комп'ютерний вірус - це невелика програма, яка написана програмістом високої кваліфікації, здатна до саморозмноження й виконання різних деструктивних дій. На сьогоднішній день відомо понад 50 тис. комп'ютерних вірусів. Дія вірусів може проявлятися по-різному: від різних візуальних ефектів, що заважають працювати, до повної втрати інформації. Більшість вірусів заражують виконавчі програми, тобто файли з розширенням .EXE та .COM, хоча останнім часом все більшої популярності набувають віруси, що розповсюджуються через систему електронної пошти.

Основними джерелами вірусів є:

- дискета, на якій знаходяться заражені вірусом файли;
- комп'ютерна мережа, в тому числі система електронної пошти та Інтернет;
- жорсткий диск, на який потрапив вірус у результаті роботи з зараженими програмами;
- вірус, що залишився в оперативній пам'яті після попереднього користувача.

Основними ранніми ознаками зараження комп'ютера вірусом є:

- зменшення обсягу вільної оперативної пам'яті;
- уповільнення роботи комп'ютера та завантаження;
- незрозумілі (без причин) зміни у файлах, а також зміни розмірів та дати останньої модифікації файлів;

- помилки під час завантаження операційної системи;
- неможливість зберігання файлів у потрібних каталогах;
- незрозумілі системні повідомлення, музичні та візуальні ефекти тощо.

Незаконні та шкідливі матеріали, що не відповідають віковим особливостям і негативно впливають на фізичне та психічне здоров'я дітей (небажаний контент)

Контент для дорослих.

Понад 95% батьків вважають найголовнішою небезпекою «дорослий» контент, який можуть переглядати діти, зокрема порноконтент. Розміри порноіндустрії неможливо навіть виміряти. Вона вважається третім великим джерелом прибутку для організованої злочинності в США, яка отримує від 8 до 10 мільйонів доларів у рік (за даними 1986 року). Інтернет може надати дітям швидкий та (у більшості випадків) безкоштовний доступ до порноконтенту. Необхідно лише ввести ключові слова або фрази для того, аби отримати тисячі посилань на сайти із дорослим контентом. Практично гарантовано, що дитина зіткнеться із порноконтентом, навіть якщо вона і не шукала його.

Пропагування сексуального насилля над дітьми, жорсткої поведінки, шкідливих звичок тощо.

Перегляд матеріалів, що містять сцени насилля та жорсткості по відношенню до людей або тварин, перешкоджає нормальному формуванню моральних цінностей та може завдати психологічних травм.

Он-лайн-зваблення дітей.

Злочинці намагаються завоювати довіру дитини, щоб втягти її в ситуацію сексуального насилля. Варто зауважити, що в сучасних ЗМІ, а також в Інтернеті, пропагується сексуальність та навіюється думка, що значимість людини залежить від її сексуальної зовнішності та поведінки. Тобто, людина розглядається як об'єкт втілення сексуальності. І злочинці цим користуються сповна. Знайомство та встановлення довіри між злочинцем та жертвою відбувається під час спілкування в мережі Інтернет: миттєві повідомлення, блоги, соціальні мережі, дошки оголошень та інше.

Діти не лише можуть легко знайти порнографічні сайти, вони так само легко можуть отримати інформацію, яка підштовхне до скоєння злочину, наприклад: інформацію про виготовлення та розповсюдження

наркотиків, способи крадіжки грошей або про те, як зробити саморобну вибухівку. Необхідно лише набрати відповідну ключову фразу і – відповідь на екрані монітора!

Кібер-хуліганство

Кібер-хуліганство – термін, який використовується для того, аби описати інформаційні атаки на дитину через Інтернет. На відміну від традиційного хуліганства, якого дитина може уникнути, знаходячись вдома, стати жертвою кібер-хуліганства можна й у власній оселі на очах у батьків. На жаль, багато дорослих навіть і не підозрюють про це.

Варіанти кібер-хуліганства досить різноманітні. Основними їх різновидами є наступні.

Кібер-булінг. Одна із форм переслідування дітей та підлітків за допомогою ІКТ. Для цього можуть створюватися сайти, на яких розміщуються матеріали, що компрометують дитину (фото, відеозйомки тощо). З метою кібер-булінгу використовуються сервіси миттєвих повідомлень, електронна пошта, соціальні мережі, ігрові та розважальні сайти, соціальні мережі, форуми та чати. Дорослі можуть здогадатися про кібер-булінг по відношенню до своєї дитини, якщо стають свідками незвичної реакції на отримані електронні листи, СМС або помічають небажання дитини відвідувати школу чи використовувати домашній комп'ютер.

Кібер-грумінг. Цей термін розкриває суть ще одного різновиду кібер-хуліганства – входження у довіру до дитини з метою використання її у сексуальних цілях. Шахраї дуже добре ознайомлені з особливостями вікової психології дитини і досить легко можуть встановлювати з нею контакт у соціальних мережах, форумах. Починаючи із віртуального спілкування та входячи у довіру до дитини, злочинці пропонують потоваришувати, а потім поступово переходять до розмов про зустріч у реальному житті та переводять тему спілкування у сексуальну площину. Як варіант, виділяють ще один вид кібер-грумінгу - наполегливе чіпляння в мережі із сексуальними пропозиціями, розмови на теми сексу, насильства та (або) виготовлення, розповсюдження і використання матеріалів зі сценами насильства над дітьми (у більшості випадків – сексуального).

Грифери. Інтернет-шахраї, які заважають учасникам он-лайн-ігор спокійно грати. Вони періодично пошкоджують ігрових персонажів,

блокують певні функції гри та викрадають як персонажів, так і їхнє віртуальне життя.

Виманювання інформації про дитину та її сім'ю з метою подальшого пограбування, шантажу.

Це відбувається завдяки використанню певних Інтернет-технологій.

Шпигунське програмне забезпечення. Це комп'ютерні програми, які збирають інформацію без відома власника комп'ютера. Зібрана інформація може містити:

- список рекламних сайтів, на які переходить користувач під час серфінгу в Інтернеті;
- особисту інформацію: ім'я, адресу та номер телефону;
- Web-сторінки, які відвідує користувач, та відомості форм, які він заповнює на цих сторінках (треба пам'ятати про обережність при повідомленні паролів своєї електронної пошти та акаунтів у соціальних мережах; не слід називати дівоче прізвище матері – подібна інформація використовується при оформленні банківських документів у якості ключових слів);
- перелік файлів, які завантажує користувач на свій комп'ютер;
- інформацію, необхідну для доступу до Інтернету: номер з'єднання модему телефонної лінії, ID та інше.

Інтернет-зловмисники можуть використовувати шпигунське програмне забезпечення, аби одночасно встановити контроль над великою кількістю комп'ютерів та використовувати їх у якості зомбі. Такі комп'ютери утворюють велику та потужну мережу, до якої можуть входити до 100 000 комп'ютерів. Ця мережа використовується шахраями для розсилання спаму, вірусів та здійснення атак на інші комп'ютери та сервери.

Фішинг – технологія Інтернет-шахрайства, розроблена з метою крадіжки конфіденційної інформації. Різновидами її є поштовий фішинг (отримання листа від «державної установи» або «банку» із вимогою повідомити особисті дані) та он-лайн-фішинг (створення ідентичної копії відомих сайтів Інтернет-магазинів з метою обманювання покупців).

Фармінг. Різновид шахрайства в Інтернеті, коли оманливим шляхом користувач потрапляє на ідентичну копію відомих сайтів. Потім

відбувається зараження комп'ютера вірусами та шпигунським програмним забезпеченням.

Он-лайн-хижаки

«Хижаки» встановлюють контакт із дітьми шляхом розмов у чат-кімнатах, обміну миттєвими повідомленнями, електронною поштою або через дошки повідомлень. Багато підлітків користуються он-лайн-форумами підтримки ровесників з метою вирішення власних проблем. Хижаки часто відвідують такі зони в он-лайні, щоб знайти вразливих жертв.

Он-лайн-хижаки виявляють по відношенню до них увагу та турботу, пропонують подарунки і таким чином намагаються поступово спокусити своїх жертв, не шкодуючи для цього ні часу, ні грошей, ні енергії. Вони в курсі найостанніших музичних новинок і все знають про хобі, які найчастіше цікавлять дітей. Вони вислуховують дітей і «співчують» їхнім проблемам. Вони намагаються позбавити комплексів молодих людей, поступово вводячи у свої розмови сексуальний контекст або показуючи відверто сексуальні матеріали.

Деякі «хижаки» працюють швидше, одразу ж втягуючи дітей у розмови на сексуальну тему. Цей більш прямолінійний підхід може включати і сексуальне домагання. Хижаки також можуть спонукати дітей, з якими вони знайомляться в он-лайні, до контакту віч-на-віч.

Найбільш вразливими для он-лайн-хижаків є молоді люди, яким притаманні такі риси:

- вони новачки в он-лайні й незнайомі з «мережевим етикетом»;
- завзяті користувачі комп'ютера;
- хочуть спробувати у житті щось нове, авантюрне;
- активно шукають уваги та дружби;
- бунтівні;
- ізольовані або самотні;
- їх приваблюють субкультури, що існують за межами їхнього власного контрольованого батьками світу.

Створення у мережі профайлів для виявлення інтересів дитини

Як зазначалося вище, соціальні мережі набувають все більшої популярності у дітей та підлітків. Більшість існуючих соціальних мереж заохочують користувачів надавати якомога більше особистої та конфіденційної інформації (прізвище та ім'я, домашня адреса, номери

телефонів, місце роботи, інтереси та нахили). Шахраю неважко обрати потенційну жертву та вивчити її за наданою у профайлі інформацією. До речі, користувачі викладають подібну інформацію у більшості випадків добровільно, не усвідомлюючи можливих наслідків такої необережності. Діти охоче розміщують фотографії, які можуть також бути використані шахраями у своїх власних цілях. Іноді підлітки охоче розміщують свої пікантні фотографії, не замислюючись над тим, що опублікована в Інтернеті інформація залишається у мережі назавжди.

Спам

Це масова розсилка комерційної, політичної та іншої реклами (інформації) або іншого виду повідомлень (у тому числі й підроблених) особам, які не висловлювали бажання їх отримувати. *Фішинг* також іноді може вважатися спамом. Метою розповсюдження підроблених повідомлень є отримання від споживачів таких особистих відомостей: власного імені та імені користувача; номера телефону й адреси; пароля або PIN-коду; номера банківського рахунку; номера дебетової або кредитної картки; коду валідації кредитної картки (CVC) або ідентифікаційного значення картки (CVV); коду соціального страхування. Таке повідомлення, зазвичай, маскується під офіційний лист від адміністрації банку. У ньому говориться, що одержувач повинен підтвердити відомості про себе, інакше його рахунок буде заблоковано, і наводиться адреса сайту, що належить спамерам, з формою, яку треба заповнити. Серед даних, які просять повідомити, є ті, що потрібні шахраям. Для того, щоб жертва не здогадалася про обман, оформлення цього сайту також імітує оформлення офіційного сайту банку чи установи. Спам також може розсилатися завдяки використанню наступних Інтернет-ресурсів.

Миттєві повідомлення

З розвитком служб миттєвих повідомлень, таких як ICQ тощо, спамери почали використовувати їх для своїх цілей. Багато з цих служб надають список користувачів, який можна використати для розсилання спаму.

Блоги, вікі

Останнім часом з'явилися Web-сайти, які можна вільно редагувати, — блоги й вікі. Наприклад, Вікіпедія створена за цією технологією. Оскільки ці сторінки відкриті для вільного редагування, на них може розміщуватися спам.

SMS-повідомлення

Спам може поширюватися не тільки через Інтернет. Рекламні SMS-повідомлення, які надходять на мобільні телефони, особливо неприємні тим, що від них важче захиститися, і одержувач іноді повинен платити за кожне повідомлення. Це може бути досить велика сума, особливо якщо абонент використовує роумінг.

Торгівля людьми

Враховуючи вищенаведені ризики, легко змодельовати декілька ситуацій в Інтернеті, які можна використати з метою торгівлі людьми: від сайтів, що пропонують роботу (роботодавці можуть виявитися звичайними торговцями людьми), до шантажу з метою викрадення жертви та її подальшого продажу.

Недостовірна інформація

Вчителі загальноосвітніх навчальних закладів помітили, що якість шкільних рефератів протягом останніх років погіршилася: інформація, яка міститься у більшості рефератів, є недостовірною, неповною або застарілою. І це не дивно, адже учні завантажують вже готові реферативні повідомлення з Інтернету та роздруковують їх. Це займає часу максимум 1 годину. Проте часто учні не замислюються над достовірністю отриманої інформації, не вміють аналізувати та узагальнювати її, тому що у них відсутнє або недостатньо розвинуте критичне мислення.

Якщо при підготовці рефератів недостовірна чи неправдива інформація до життєвого ризику не призводить, то у випадку пошуку інформації, що стосується здоров'я, ризик істотно збільшується. Проблеми, що стосуються здоров'я, як фізичного, так і психічного, повинні обговорюватися лише у родині, із дорослими та фахівцями. В Інтернеті на різноманітних форумах досить легко знайти (і ми знаходили) інформацію, яка є не лише антинауковою, а й життєво небезпечною, якщо нею скористатися.

РОЗДІЛ ІІІ. ПРЕВЕНТИВНА РОБОТА, СПРЯМОВАНА НА ВИХОВАННЯ КУЛЬТУРИ ТА БЕЗПЕЧНОЇ ПОВЕДІНКИ КОРИСТУВАЧА ІНТЕРНЕТУ

Актуальність проблеми **безпеки дітей та молоді в Інтернеті** не викликає жодного сумніву. Ми провели аналіз профілактичних програм, що передбачають формування навичок безпечної поведінки у мережі, і дійшли висновку, що на сьогодні реально дієвою профілактичною програмою є програма «Онляндія – безпека дітей в Інтернеті».

1. Діяльність Коаліції за безпеку дітей в Інтернеті

Програма «Онляндія – безпека дітей в Інтернеті» ініційована Коаліцією за безпеку дітей в Інтернеті, що заснована компанією «**Майкрософт Україна**» у 2008 році в рамках програми «Партнерство у навчанні». Членами Коаліції є 27 організацій, серед яких неурядові організації: Всеукраїнська мережа протидії комерційній сексуальній експлуатації дітей (член міжнародної організації ЕКПАТ), Міжнародна Школа Рівних Можливостей, Міжнародний центр захисту дітей від експлуатації та викрадень, Міжнародний дитячий фонд ООН (ЮНІСЕФ), Міжнародна організація з міграції, Міжнародний жіночий правозахисний центр «Ла Страда – Україна», Інститут інформаційного суспільства, Інтернет-Асоціація України, проект «Відкритий світ інформаційних технологій» (IDEA), Американська Торгівельна Палата в Україні, ряд міністерств та відомств України, компанії «Майкрософт Україна», «Хьюлетт-Пакард», «Воля», телекомунікаційна група Vega, комунікаційна група ESG, «ПрессКом», «Астеліт» (торгова марка life:), платіжна система WebMoney, «Укртелеком» (торгова марка «ОГО!»), «Київстар», «МакДональдз Україна», компанія МТС, видавництво «Едіпрес Україна», «Гала-радіо» та громадський діяч і музикант Святослав Вакарчук, який є засновником фонду «Люди Майбутнього».

Програма «Онляндія – безпека дітей в Інтернеті» включає цілий ряд заходів, спрямованих на навчання дітей, вчителів та батьків правилам безпечного користування Інтернетом.

Однією з найважливіших ініціатив Коаліції є програма для шкіл «Безпека дітей в Інтернеті», в рамках якої, починаючи з 2008 року,

тренери-волонтери провели 2586 тренінгів для близько 64 тисяч дітей та підлітків, а також більше 19 тис. вчителів і батьків.

Першим кроком Коаліції став запуск у квітні 2008 року Web-сайту «Онляндія – безпечна Web-країна» www.onlandia.org.ua. На цьому сайті представлені матеріали для дітей, їхніх батьків та вчителів: інтерактивні ігрові сценарії, короткі тести, розробки уроків, завдяки яким діти та дорослі зможуть засвоїти основи безпечної роботи в Інтернеті. Також сайт пропонує зрозумілу та перевірену на практиці інформацію про Інтернет-безпеку, після ознайомлення з якою навіть користувачі-початківці зможуть ефективно використовувати ресурси мережі та захистити себе від небажаного контенту. Популярність сайту постійно зростає, щомісяця його відвідують до 7 тис. унікальних користувачів, отже, все більшій кількості людей вдається отримати інформацію про проблему захисту від шкідливої інформації та зробити перші кроки до поліпшення ситуації.

У 2008 році Коаліція також ініціювала та провела у приміщенні Верховної Ради України круглий стіл, присвячений темі безпеки дітей в Інтернеті. У заході взяли участь представники державних органів влади, неурядових організацій та громадські діячі. Результатом обговорення проблеми стало прийняття резолюції, яку було передано на розгляд у Верховну Раду України, а також відповідні міністерства та відомства, з метою отримання допомоги у реалізації програми «Онляндія – безпека дітей в Інтернеті». У резолюції зазначено ряд змін, які рекомендовано внести у законодавство України. Це дозволить боротися з розповсюдженням і виробництвом дитячої порнографії та сексуальним туризмом, які дедалі більше поширюються через недосконалість законодавчої бази.

Під час проведення круглого столу представники правоохоронних органів підкреслили, що великою проблемою у вирішенні питання безпеки дітей в Інтернеті є недостатня кількість ресурсів та засобів для відстеження кібер-злочинців та Інтернет-небезпек. Через це Інтерпол та Міжнародний центр захисту дітей від експлуатації та викрадень за підтримки компанії «Майкрософт Україна» провели тренінги-семінари для працівників Міністерства внутрішніх справ України, спрямовані на пошук шляхів ліквідації кібер-злочинності. Метою семінарів було забезпечення правоохоронних органів технічними засобами для розслідування справ, пов'язаних з експлуатацією дітей в Інтернеті.

У лютому 2009 року Коаліція за безпеку дітей в Інтернеті провела масштабну соціальну кампанію «Місяць безпечного Інтернету». Присвячена європейському Дню безпечного Інтернету, кампанія включала такі заходи: соціальну рекламу, інформаційно-розважальний марафон у великих містах України, он-лайн-петицію «Так! безпечному Інтернету для дітей в Україні» та запуск безпечної електронної пошти для дітей.

Соціальну рекламну кампанію «Інтернет. Реальніше, ніж ти думаєш» підтримали телевізійні канали, друковані ЗМІ, он-лайн-ресурси та зовнішні носії. Основна ідея заходу – показати, що до інформації в Інтернеті мають доступ мільйони незнайомих, які можуть використовувати її, як завгодно, тому не слід розповсюджувати особисті дані у відкритому доступі. До програми долучилася агенція Think! McCann Erickson, яка розробила концепцію реклами, та продакшн-студія Radioactive Film (режисер – Іван Сауткін), яка створила рекламний відеоролик. Свій внесок у соціальну кампанію зробили також журнали «ТЗ», «Домашній ПК», «Mobility», «Шпиль!» та «SMS», що розмістили друковану рекламу, та телевізійні канали «5 Канал» і «MTV Україна», які демонстрували відеоролики в ефірі.

Учасники марафону, що проходив під девізом «Прийди й зроби крок до безпечного Інтернету» з 10 по 14 лютого 2009 року у великих містах України, дізналися, як використовувати усі переваги віртуального простору, не наражаючись при цьому на небезпеку. Марафон підтримала молода зіркова група Chicos de la fiesta, а також Гала-радіо. У кожному місті проводився флеш-моб – одночасний символічний крок усіх учасників через натягнуту стрічку безпеки. Участь у марафоні взяли понад 2000 школярів у 5-и містах України.

Ще одним кроком кампанії «Місяць безпечного Інтернету» став запуск першого в Україні спеціального поштового сервісу для дітей - безпечної електронної пошти «Онляндія». Електронна пошта створена на сайті «Онляндія» (www.onlandia.org.ua) і базується на безкоштовному Web-сервісі Microsoft – Windows Live Mail. Інтерфейс поштового домену @onlandia.org.ua не містить реклами, а електронна скринька захищена від несанкціонованого спаму та вірусів. При цьому підлітки можуть не тільки надсилати електронні листи, але й спілкуватися з друзями в режимі он-лайн за допомогою сервісу обміну миттєвими повідомленнями.

У 2010 році головні ініціативи Коаліції за безпеку дітей в Інтернеті були спрямовані на навчання батьків ключовим правилам захисту їхніх дітей від реальних загроз віртуального світу. Першим кроком до цього стала відкрита освітня конференція для батьків, що відбулася 9 лютого 2010 року у Києві. Сайт «Онляндія» у лютому поповнився новим розділом «Клуб Інтернет-батьків», а також навчальними модулями, з яких батьки зможуть дізнатися більше про використання соціальних мереж і важливість захисту приватної інформації під час он-лайн-спілкування. 9 лютого 2010 року, у День безпечного Інтернету, заходами, спрямованими на он-лайн-безпеку дітей, було охоплено понад 300 населених пунктів по всій країні.

2. Захист дітей та молоді від негативних інформаційних впливів – один із напрямів української державної політики в галузі освіти

Змістом державної політики у сфері захисту суспільної моралі є створення необхідних правових, економічних та організаційних умов, які сприяють реалізації права на інформаційний простір, вільний від матеріалів, що становлять загрозу фізичному й інтелектуальному розвитку або морально-психологічному стану дітей та молоді. Питанню захисту молодого покоління від негативних інформаційних впливів приділяється значна увага.

Згідно з чинним законодавством України, виробництво, поширення, використання матеріалів із зображенням сексуального насилля над дітьми та втягнення неповнолітніх до виготовлення порнографії карається позбавленням волі на строк від 3 до 7 років.

Нормативно-правові документи, прийняті в галузі освіти, відповідають статті 6 «Освіта дітей» Конвенції Ради Європи про захист дітей від сексуальної експлуатації та сексуальних домагань та пункту 62 Пояснювальної записки до неї в частині отримання дітьми дошкільного та шкільного віку відповідної інформації із зазначених питань.

Вивчення теми безпечної роботи в Інтернеті здійснюється відповідно до чинних програм зі шкільних курсів «Інформатика» та «Основи здоров'я», а саме:

- навчальної програми з інформатики для 9-12 класів загальноосвітніх навчальних закладів. Академічний рівень (авт.: Завадський І.О., Потапова Ж.В., Дорошенко Ю.О.);
- навчальної програми з інформатики для 9-12 класів загальноосвітніх навчальних закладів. Рівень стандарту (авт.: Завадський І.О., Потапова Ж.В., Дорошенко Ю.О.);
- навчальної програми з інформатики для вечірньої середньої загальноосвітньої школи (авт.: Литвинова С.Г., Проценко Т.Г.)
- навчальної програми з курсу «Основи здоров'я» для 5-9 класів загальноосвітніх навчальних закладів (авт. Бойченко Т.Є., Заплатинський В. М., Дивак В.В.).

Вивчення питань прав та свобод дітей з отримання інформації та захисту від негативних інформаційних впливів передбачено навчальними програмами з курсів «Правознавство» (10-12 кл.) та «Людина і світ» (12 кл.).

Навчальною програмою шкільного курсу «Основи здоров'я» для 1-4 класів загальноосвітніх навчальних закладів передбачено вивчення питань безпечної поведінки дитини в соціальному середовищі з 1 класу (авт. Бойченко Т.Є., Заплатинський В. М., Дивак В.В.).

Міністерство освіти і науки, молоді та спорту проводить інформаційно-просвітницьку роботу з питань безпечної роботи в Інтернеті, співпрацює із державними, бізнесовими структурами, неурядовими організаціями. Наведемо лише декілька прикладів такої співпраці.

Компанія «Майкрософт Україна» виступила з ініціативою щодо створення «Коаліції за безпеку дітей в Інтернеті», яку підтримало міністерство (лист ІТЗО МОН України від 28.04.09 № 1.4/18-1431). Адміністративно підтримується також розроблена компанією програма «Онляндія – безпечна Web-країна». У загальноосвітніх навчальних закладах започатковано вивчення базового курсу для вчителів і батьків «Курс цифрових технологій», ініціатором впровадження якої також виступила компанія «Майкрософт Україна».

З 15 жовтня по 15 лютого 2010 року завдяки підтримці компанії МТС у школах України були проведені Уроки мобільної грамотності для 60 000 школярів-старшокласників. Вчителі та учні отримали посібники, що допоможуть грамотно і безпечно використовувати Інтернет та мобільний зв'язок для навчання та дозвілля.

Завдяки підтримці компанії «Майкрософт Україна» та компанії Інтел у 2009 році у загальноосвітніх навчальних закладах розпочалася реалізація науково-педагогічного проекту «1 учень - 1 комп'ютер» (наказ МОН України від 2 лютого 2009 року № 54 «Про проведення дослідно-експериментальної роботи з теми: «Науково-методичні основи використання ІКТ у навчально-виховному процесі в середовищі «1 учень – 1 комп'ютер» на базі шкільних нетбуків»). У рамках цього проекту розроблено підготовчий курс для учнів 1 класу, яким передбачено вивчення правил безпечного користування Інтернетом.

3. Загальні методичні рекомендації. Формування у дітей компетенцій безпечного користування ресурсами мережі Інтернет

Коли ми говоримо про безпечну поведінку у мережі Інтернет, то маємо на увазі, що користувач «озброєний» необхідними знаннями та навичками. Навіть якщо підліток начебто впевнений у правильності своїх дій під час роботи в мережі Інтернет, часто його вчинки свідчать про протилежне.

На власному досвіді роботи та успішному досвіді колег ми переконалися, що у формуванні навичок впевненої та безпечної поведінки дітей у мережі Інтернет найбільш позитивний результат дає тренінгова діяльність.

Тренінг (англ. *training* від *train* — навчати, виховувати) – це короткостроковий захід або декілька заходів, направлених на отримання знань, набуття навичок, накопичення власного досвіду.

Під час тренінгу учні мають можливість не лише почути про ризики та небезпеки в Інтернеті, а й пережити змодельовані ситуації. Вчитель не дає готових відповідей на питання, а лише спрямовує дітей до прийняття логічно обґрунтованого рішення. Найважливіше, що під час тренінгу дитина самостійно приймає виважене рішення, яке найбільш цінне, оскільки є власним «відкриттям» дитини, а тому має більше шансів бути втіленим у життя.

Інтерактивна методика тренінгової програми ґрунтується на переконанні, що люди ефективніше засвоюють матеріал, якщо розуміють значення своїх власних знань та досвіду і мають змогу поділитися ними в комфортному середовищі.

Програма тренінгу повинна бути побудована таким чином, щоб надана інформація підкріплювалася практичними діями. Різноманітність методів, що використовуються в інтерактивних тренінгах, пояснюється особливостями сприйняття людини. Почнемо з того, що мозок людини отримує та переробляє, тобто усвідомлює, інформацію у певний спосіб. Спочатку людина переймає ДОСВІД у вигляді теоретичної інформації. Далі наводиться ПРИКЛАД використання цього досвіду на підтвердження наданої інформації. Наступний крок – ЗАСТОСУВАННЯ - використання людиною отриманого досвіду для вирішення власної проблеми. Далі йде УЗАГАЛЬНЕННЯ – це коли людина окреслює коло проблем, які можуть бути вирішені через застосування отриманого досвіду.

Отже, кожен з блоків інформації подається за схемою:



Метою проведення тренінгу з безпечного використання мережі Інтернет є надання слухачам достатнього обсягу знань та інформації з цього питання.

Цільові групи, для яких призначена програма тренінгу, - школярі та молодь, котрі користуються мережею Інтернет, батьки учнів і викладачі загальноосвітніх навчальних закладів.

Інтерактивні методики викладання, які застосовуються на тренінгах, ґрунтуються на наступних принципах.

Принцип активності

Активність учасників тренінгової групи відрізняється від активності людини, яка слухає лекцію або читає книгу. На тренінгу люди заохочуються до оволодіння матеріалом різними способами, серед яких – використання ігрових форм.

Це може бути «програвання» тієї чи іншої ситуації (рольова гра), форум-театр, спостереження за поведінкою інших за спеціальною схемою тощо.

Активність учасників тренінгу підвищується, якщо ми даємо їм установку на готовність включитися в діяльність у будь-який момент. Особливо ефективними є ті ситуації та вправи, які дозволяють усім членам групи брати в них участь одночасно.

Принцип активності спирається на відому з експериментальної психології ідею, згідно з якою людина засвоює:

- 10% прочитаного,
- 20% почутого,
- 30% побаченого,
- 50% почутого та побаченого,
- 70% проговореного,
- 90% проговореного і виконаного.

Принцип дослідницької (творчої) позиції

Суть цього принципу полягає в тому, що у процесі тренінгу його учасники усвідомлюють уже відомі ідеї, знаходять закономірності, а також, що є особливо важливим, відкривають свої власні ресурси, можливості та особисті якості.

Щоб активізувати аудиторію, тренер виступає в ролі режисера: «організовує» такі ситуації, які б дали можливість присутнім усвідомлювати, апробувати і тренувати нові способи (стилі) поведінки, позбутися комплексів і набути впевненості.

Реалізація цього принципу часом може зустріти певний супротив з боку аудиторії, якщо така форма навчання є незвичною для когось із учасників. Подолати таку реакцію допоможуть запропоновані тренером для обговорення (або «програвання») у групі «проблемні ситуації», які дозволять учасникам поекспериментувати, моделюючи свою поведінку та творчі підходи і до життєвих ситуацій, і до себе.

Принцип усвідомлення поведінки

У процесі набуття знань поведінка учасників переводиться зі спонтанно-імпульсивного на усвідомлений рівень. Універсальним засобом для цього є так званий зворотній зв'язок. Тому створення умов для ефективного зворотнього зв'язку – одне з першочергових завдань тренерської роботи.

Принцип партнерського спілкування

Партнерським спілкуванням називається таке спілкування, коли визнається цінність кожної особистості, враховуються інтереси всіх учасників, з розумінням сприймаються їхні реакції: почуття, емоції, переживання.

Дотримання принципу партнерського спілкування створює в групі атмосферу розкнутості, довіри, щирості, що дозволяє присутнім вільно імпровізувати зі своєю поведінкою, не соромлячись можливих помилок. Ці засади тісно пов'язані з принципом творчої, дослідницької позиції учасників групи. Послідовна реалізація вищеназваних принципів – одна з умов ефективної роботи групи на тренінгу. Саме це робить тренінгову методику інноваційно-відмінною від інших форм навчання.

Таким чином, вчителю необхідно врахувати наступні ключові аспекти формування в учнів компетенцій і навичок безпечної поведінки в мережі Інтернет.

1. Педагог повинен чітко зрозуміти для себе, що саме повинен отримати кожен учасник тренінгу після його завершення. **Мета** повинна бути реалістичною, конкретною та позитивною. Вчитель не може поставити перед собою занадто узагальнену мету: навчити дітей правилам безпеки в Інтернеті. Але він може навчити, наприклад, шести правилам безпечної роботи в мережі. При цьому вчитель планує досягти чогось позитивного (навчити, показати, сформувати стійку мотивацію). Якщо мета конкретна і позитивна, вона буде реалістичною.

2. Хороший тренінг орієнтований на подолання можливих ризиків у мережі Інтернет, а не на те, щоб «посяяти» переживання та хвилювання через ці ризики. Як би добре нас не навчали, ми все ж робимо іноді помилки. До цих помилок необхідно ставитися як до життєвої реальності. Адже у чутливої та емоційної людини, особливо підлітка, ці помилки можуть перерости у великі проблеми. Людина починає витрачати величезну кількість енергії та часу на хвилювання та переживання через допущені помилки, не рухаючись до самої мети.

3. Необхідно виховувати адекватну реакцію на мінливу ситуацію, що виникає в реальному житті, за допомогою Інтернету. Адже Інтернет — ідеальне місце для досить швидкої «зміни декорацій». Тому треба бути готовим до частоті зміни «декорацій» у житті і не робити з цього життєвої проблеми.

4. Необхідно вчити дітей жити реальним життям, а не віртуальним. Під час тренінгу корисно акцентувати увагу учнів на тому, що набагато легше заховатися за будь-яку соціальну роль (віртуальний образ) і навіть вжитися в цю роль у віртуальному світі. Але життя навколо не віртуальне, а реальне.

5. Важливо правильно соціально орієнтувати підлітків. Практично всі вони користуються Інтернетом. Необхідно показати, що вико-

ристання нелегальних чи шкідливих ресурсів Інтернету може призвести до асоціальної поведінки. Тому так важливо зорієнтувати підлітків на побудову конструктивних відносин з людьми, направити їх до людей, а не від людей або проти них.

6. Узагальнюючи блок методичних рекомендацій, звертаємо увагу педагогів на важливість формування в учнів **стійкої мотивації** до безпечної поведінки під час роботи в мережі Інтернет. Під час тренінгової діяльності необхідно акцентувати увагу на наступних компонентах формування мотивації.

Цільовий компонент. Одним з головних принципів профілактики негативних інформаційних впливів на молодь є надання широкого вибору безпечної поведінки. У молоді повинен бути вибір: або не користуватися Інтернетом, або ж користуватися розумно. Звісно, всі обирають останній варіант. Але право вибору повинно бути.

Змістовий. Кожна програма тренінгу повинна мати чіткий зміст та враховувати особливості аудиторії, для якої вона призначена: вік, стать, рівень соціальної культури, рівень поінформованості, ступінь ризикованої поведінки, соціальне оточення та умови життя.

Операційно-дійовий. Ефективність програми та кінцевий результат тренінгу залежить від вдалого поєднання різноманітних методів: обговорення у групі, мозковий штурм, форум-театр, рольові ігри, моделювання поведінки із наступним аналізом, дискусії, практичне застосування життєвих навичок, складання схеми-плану поведінки у ризикованих ситуаціях під час перебування у мережі Інтернет. Переваги активного навчання полягають у тому, що вони стимулюють співробітництво, а не змагання. Людина починає краще сприймати інших, у неї підвищується почуття власної гідності, розвивається розуміння потреб інших, толерантність.

Стимулюючо-мотиваційний. Ефективність програми тренінгу залежить саме від реалізації цього компонента. Позитивна мотивація до роботи можлива лише за умови врахування особливостей цільової аудиторії та закріплення змісту програми інтерактивними методами.

Контрольно-регулюючий. Цей компонент дозволяє коригувати знання за допомогою різноманітних методів безпосередньо під час самого тренінгу.

4. Підготовка педагогів-тренерів з безпеки в Інтернеті

4.1. Загальні методичні рекомендації

Необхідно зауважити, що результативність превентивної роботи тренерів-педагогів залежить не лише від рівня їхньої поінформованості щодо даної проблематики, а й від їхньої мотивації. Педагог, який усвідомлює актуальність питання безпеки дітей в Інтернеті та сам вільно володіє як теоретичним, так і практичним матеріалом, зможе сформуванати у дітей стійку мотивацію до безпечної поведінки під час перебування у мережі Інтернет.

Ми вважаємо, що лише методичних рекомендацій та консультацій для підготовки тренерів недостатньо: потрібне поєднання формальної та неформальної форми освіти. Тільки повноцінний **тренінг** із усіма обов'язковими атрибутами та методиками проведення дозволить отримати необхідний результат. Педагог, який сам пройшов через тренінгову діяльність, відчув на собі сенс тренінгових методик, зможе правильно та, найголовніше, результативно передати учням важливу інформацію про ризики та небезпеки в Інтернеті.

Керуючись практичним досвідом, ми виділяємо наступні основні **правила групової роботи під час підготовки педагогів-тренерів з Інтернет-безпеки**:

1. **Тут і зараз.** Вікові особливості педагогів іноді заважають кращому засвоєнню необхідного матеріалу: дорослі досить легко переключаються на інші, більш важливі або цікаві для них питання: економічний стан держави, рівень заробітної платні тощо. Тому цей принцип допомагає орієнтувати усіх учасників таким чином, щоб предметом їхнього аналізу були саме ті процеси, які відбуваються у групі в цей момент.

2. **Відкритість.** Тренер, використовуючи різноманітні техніки, створює атмосферу «відкритості», коли кожен учасник почуває себе впевнено у висловлюванні власних думок. Це правило сприяє налагодженню зворотнього зв'язку, тобто тієї інформації, яка має важливе значення для запуску механізмів самосвідомості та міжособистісної взаємодії.

3. **Принцип «Я».** Основну увагу необхідно зосереджувати на процесах самопізнання, самоаналізу та рефлексії. Тренер групи повинен слідкувати, аби учасники висловлювалися від свого імені. Це досить

важливий момент, бо на даному етапі вирішується одне із завдань тренінгу – навчити умінню брати на себе відповідальність.

4. Активність. Навіть якщо вправа має лише демонстраційне значення, кожен учасник має право та можливість висловити свої враження.

5. Конфіденційність. Учасниками подібних тренінгів є, переважно, люди, відомі у суспільстві: керівники навчальних закладів, викладачі, лідери громадських організацій. Все, що відбувалося під час тренінгу, не повинно стати відомим широкому колу людей. Особиста інформація учасників тренінгу, їхні враження про інших, фотографії – все це не повинно бути оприлюднено без їхнього дозволу.

Досить часто початок тренінгів характеризується апатичністю учасників. Вони або втомлені, або не налаштовані на результативну роботу. Іноді на початку тренінгу можна почути, що учасники хочуть просто прослухати потрібну інформацію. У таких випадках ні в якому разі не можна йти на поступки учасникам та піддаватися їхнім умовлянням. Досвідчений тренер зуміє провести тренінг таким чином, аби всі взяли в ньому активну участь. До речі, показником успіху тренінгу є показник поживлення «холодних» та «апатичних» учасників під час роботи у групі. Завдяки правильній організації тренінгу саме такі учасники і стають потім найбільш активними та ініціативними.

Таким чином, аби запобігти виникненню подібних ситуацій у роботі тренінгу, ще на його початку необхідно обов'язково планувати модуль *«Створення мотивації до діяльності»* (дивись додаток). Бажано провести одну-дві вправи з метою створення у групі робочого настрою. Вправи цього модуля дають можливість учасникам забути про те, що їх може турбувати в цей час, і зосередитися на ситуації «тут і зараз». Тренер матиме змогу вирівняти загальний емоційний фон групи: хтось мобілізується, а дехто заспокоїться. Отже, ці вправи допоможуть налаштувати групу на плідну роботу заради гарного результату.

Під час планування тренінгу для майбутніх тренерів, які незнайомі між собою, необхідно запланувати модуль *«Знайомство»*. Будь-яке спілкування розпочинається із знайомства. Так і тренінгова взаємодія неможлива без вправ на пізнання один одного, вправ, які допомагають запам'ятати ім'я кожного учасника та дізнатися більше один про одного.

Під час реалізації цього модуля тренер має можливість отримати чимало інформації про учасників:

- тренер помічає для себе, яке ім'я учасник собі обирає, наприклад, Тетяна, Танюша або Тетяна Петрівна. Найкращий результат тренер отримує тоді, коли звертається до учасника, називаючи ім'я, яке найбільш прийнятне для нього;

- тренер виокремлює для себе деякі особистісні риси учасників: сором'язливість, демонстративність тощо;

- тренер отримує інформацію про загальний емоційний фон групи та учасників.

Будь-яка вправа (дивись додаток) може мати багато варіантів, які будуть відрізнятися як за змістом, так і за формою проведення, тому необхідно творчо підійти до кожної запропонованої вправи і пам'ятати, що дуже результативною буде ігрова взаємодія.

Під час формулювання правил поведінки на тренінгу слід врахувати наступне:

- правила поведінки формулюють самі учасники;
- необхідно включити пункт «перевести мобільний телефон у режим вібрації»;

- обов'язково включити пункт «покарання». Наприклад, це може бути купівля великої коробки цукерок під час останньої перерви на каву. Ні в якому разі не можна пропонувати та затверджувати «покарання», які можуть принизити гідність учителя.

При підготовці вправ на формування мотивації до безпечної поведінки в мережі Інтернет необхідно врахувати теоретичний та практичний досвід користування ресурсами Інтернету учасників тренінгу. Якщо немає можливості попередньо поспілкуватися з учасниками, то це можна з'ясувати під час презентації діяльності груп, яка спрямована на узагальнення корисних ресурсів та ризикованих ситуацій в Інтернеті. Аналіз результатів діяльності педагогів дозволить тренеру зробити висновок про рівень оволодіння ними ІКТ-компетенціями.

Дуже важливими є етап формулювання правил поведінки у мережі Інтернет. Досвід свідчить, що мотивація до безпечної поведінки найкраще формується у тому випадку, коли учасники САМОСТІЙНО формулюють та узагальнюють ці правила. Тренер не повинен називати жодного правила поведінки в мережі Інтернет до етапу презентації учасниками цих правил. Після презентації тренер проводить узагальнення всіх сформульованих правил та детально зупиняється на кожному з них. Після цього необхідно наголосити на тому, що не тренер

сформулював правила, а учасники самостійно це зробили. На цьому етапі дуже корисно провести аналогію з дітьми підліткового віку. Діти не сприймають правил, які нав'язуються дорослими. Але завжди дотримуються правил, які самостійно прийняли після певного реального життєвого досвіду.

Для досягнення більшої результативності у підготовці педагогів-тренерів бажано розробити із учасниками програму з безпеки дітей в Інтернеті для свого навчального закладу. Під час підготовки цієї програми рекомендуємо скористатися наступним шаблоном:

- мета програми;
- завдання програми;
- конкретні практичні заходи, спрямовані на відпрацювання навичок безпечної поведінки;
- перелік наявних ресурсів (фахівці, приміщення, обладнання, канцтовари, апаратура тощо);
- перелік відсутніх ресурсів (як ми можемо отримати ці відсутні ресурси?).

Дуже корисним та необхідним вважаємо етап презентації учасникам тренінгу освітніх ресурсів, які допомагають педагогам впроваджувати сучасні ІКТ у навчально-виховний процес. Перелік цих ресурсів знаходиться у додатках.

Логічним завершенням тренінгу є узагальнення матеріалу. Тренер проводить узагальнення на кожному етапі, не зупиняючись на окремих деталях. Головне - наголосити на ключових моментах. Наприклад: «Сьогодні ми говорили про значення Інтернету в житті молоді, про його користь та ризики, дізналися про шляхи формування у молоді мотивації до безпечної поведінки у мережі Інтернет, а також почули про корисні для освітян ресурси, які допомагають зробити навчально-виховний процес більш якісним та продуктивним».

4.2. Структурно-логічна модель підготовки педагогів-тренерів з безпеки в Інтернеті

1	Мета тренінгової програми	Підготовка педагогів-тренерів з безпеки дітей в Інтернеті	
2	Перелік конкретних завдань тренінгової програми:	1. Озброїти учасників знаннями про ризики в Інтернеті. 2. Сформувати в учасників розуміння необхідності дотримуватися певних правил поведінки в Інтернеті. 3. Сформувати навички користування правилами безпечної поведінки в Інтернеті. 4. Озброїти учасників знаннями про шляхи формування у дітей стійкої мотивації до безпечної поведінки у мережі Інтернет	
3	Цільова група, категорія учасників:	Студенти-педагоги, вчителі, вихователі, соціальні працівники по роботі з молоддю, шкільні психологи.	
4	Кількість учасників тренінгового заняття:	15-25	
5	Час, необхідний для проведення тренінгу:	7 годин	
6	Структура тренінгу		
	Вид діяльності	Опис діяльності	Тривалість
	Вступ	Тренер розповідає учасникам про програму «Онляндія - безпека дітей в Інтернеті», повідомляє тему та мету тренінгу	5 хв.
	Мотивація до діяльності	Вправа на формування в учасників мотивації до активної та плідної участі у тренінгу	15 хв.
	Очікування	Вправа на визначення очікувань учасників тренінгу	5 хв.

Правила	Група під керівництвом тренера обговорює та приймає правила поведінки під час тренінгу	5 хв.
Знайомство	Кожен учасник називає своє ім'я та коротко розповідає про свій досвід користування Інтернетом	10 хв.
Інформативний блок №1. ІКТ у сучасному світі та в Україні.	Із використанням презентації PowerPoint тренер інформує про проникнення Інтернету у всі сфери життєдіяльності суспільства.	10 хв.
Групова діяльність	Учасники, об'єднавшись у 2 групи, готують по одній презентації: користь Інтернет-ресурсів та ризики від Інтернет-ресурсів.	15 хв.
	Презентація групової діяльності. Узагальнення інформації тренером.	10 хв.
Перерва		15 хв.
Інформативний блок №2. Ризики та небезпеки віртуального простору. Результати дослідження в Україні.	Із використанням презентації PowerPoint тренер інформує про результати досліджень в Україні, акцентуючи увагу на конкретних ризиках та небезпеках у мережі Інтернет.	20 хв.
Мозковий штурм	Тренер пропонує для обговорення проблемне запитання: «Що робити для вирішення цієї ситуації в Україні?». Обговорення.	15 хв.
Рухавка	Вправа на підвищення рівня взаємодії в групі (дивись додаток).	5 хв.

<p>Інформативний блок №3. Тренінгова діяльність – запорука формування у дітей стійкої мотивації до безпечної поведінки в Інтернеті.</p>	<p>Інформування учасників: 1. Чому саме тренінг? 2. Структура тренінгу. 3. Особливості тренінгових технологій в залежності від цільової аудиторії.</p>	<p>45 хв.</p>
<p>Перша</p>		
<p>Інформативний блок №3. Вікові особливості учасників.</p>	<p>Інформування учасників про вікові особливості цільової аудиторії, для якої готується тренінг.</p>	<p>45 хв.</p>
<p>Групова діяльність</p>	<p>Учасники, об'єднавшись у 3 групи, готують по одній презентації: вікові особливості дітей 7-11 років, 12-15 років, 17-19 років, дорослих віком від 30 до 40 років.</p>	<p>10 хв.</p>
<p>Презентація діяльності.</p>		
<p>Інтерактивна діяльність Формування мотивації до безпечної поведінки у мережі Інтернет</p>	<p>Вправа на формування стійкої мотивації до безпечної поведінки у мережі Інтернет: - під час спілкування у соціальних мережах; - під час обміну миттєвими повідомленнями; - під час обміну фотографіями на іншій особистою інформацією; - під час користування Інтернет-магазинами; - при користуванні електронною поштою; - при потраплянні на сайти з дорослим контентом та контентом, який є небажаним для дітей.</p>	<p>60 хв.</p>
<p>Групова діяльність. Правила безпечного користування Інтернетом</p>	<p>Учасники, об'єднавшись у дві групи, готують презентації правил безпечного користування Інтернетом для дітей віком 7-11 років (або за вибором учасників).</p>	<p>15 хв.</p>

Перерва			
	Групова діяльність. Практичні засади впровадження програми «Онляндія- безпека дітей в Інтернеті» у навчально-виховний процес	Учасники, об'єднавшись у 2 групи, готують презентації ідей щодо практичного впровадження у навчальному закладі програми з безпеки дітей в Інтернеті Презентація програми.	15 хв. 15 хв.
	Інформативний блок №4. Освітні ресурси для вчителів	Презентація освітніх ресурсів Web 2.0 для вчителів.	20 хв.
	Узагальнення	Тренер узагальнює результати тренінгу.	5 хв.
	Вправа на узагальнення	Вправа на узагальнення матеріалу (дивись додаток).	10 хв.
7	Обладнання:	Тренінг проводиться у просторому приміщенні. Стільці розташовані по колу із достатнім для вправ простором посередині. Фліпчарт, маркери різнокольорові, папір А-4, проектор, ноутбук, стікери, кольоровий папір, клей, скотч.	
8	Оцінка тренінгу (критерії успіху):	Результати тренінгу можна відслідкувати за висловлюваннями учасників під час підбиття підсумків і презентації системи впровадження програми з безпеки дітей в Інтернеті у навчально-виховний процес.	
9	Додатки та роздатковий матеріал:	Сувенірна та поліграфічна продукція з символікою та інформацією «Онляндії», картки із ситуаційними завданнями.	

5. Організація навчально-виховної роботи з дітьми 7-10 років

5.1. Вікові психофізіологічні особливості

Плануючи превентивну роботу з дітьми, необхідно враховувати особливості розвитку їхніх вікових психічних процесів.

Вікові особливості пам'яті. Під впливом навчання формується логічна пам'ять, яка має вирішальне значення для здобуття знань. Але не вміючи ще диференціювати завдання (запам'ятати і відповісти) від інших навчальних завдань (зрозуміти тощо), молодші школярі виробляють у себе настанову на дослівне запам'ятовування і відтворення. За умови правильного педагогічного керівництва учні *осмислено* запам'ятовують доступний для них матеріал. Проте *дослівне* запам'ятовування й відтворення має і позитивне значення. Воно є важливим засобом накопичення словникового запасу і розвитку культури дитячого мовлення та довільної пам'яті. Розвиток пам'яті полягає у зміні співвідношення між мимовільним і довільним запам'ятовуванням (зростає довільне), формуванні образної та словесно-логічної пам'яті. Для розвитку логічної пам'яті важливою є настанова вчителя: зрозуміти (проаналізувати, порівняти, співвіднести, згрупувати тощо) матеріал, завчити його. Довільне запам'ятовування продуктивне тоді, коли запам'ятований матеріал стає змістом активної діяльності учнів.

Вікові особливості уяви. Розвиток уяви відбувається у напрямі від репродуктивних її форм до творчого осмислення уявлень, від довільного їх комбінування до логічно обґрунтованої побудови нових образів. Зростає вимогливість дітей до витворів їхньої уяви, швидкість побудови образів фантазії.

Вікові особливості процесу мислення. Мислення стає конкретно-образним, але все більшого значення набувають абстрактні компоненти. Під впливом навчання змінюються співвідношення між його образними і понятійними, конкретними та абстрактними компонентами. Молодші школярі швидше оволодівають індуктивними умовиводами, ніж дедуктивними.

Емоції молодшого школяра. Джерелом емоцій у молодших школярів є навчальна та ігрова діяльність. Формуванню почуттів сприяють успіхи та невдачі у навчанні, взаємини в колективі, читання художньої літератури, сприймання телепередач, кінофільмів, інтелектуальні ігри тощо. До емоційної сфери належать переживання

нового, здивування, сумнів, радощі пізнання — це основи формування пізнавальних інтересів, допитливості учнів. Колективні заняття сприяють розвитку моральних почуттів і формуванню таких рис характеру, як відповідальність, товариськість, колективізм. Необхідно враховувати, що молодші школярі емоційно вразливі. Відбувається диференціація сором'язливості, яка виявляється в реагуванні на людину, думка якої має значення для них. Розвивається почуття самолюбства, що виявляється в гнівному реагуванні на приниження їхньої гідності й позитивне емоційне переживання у випадку визнання їхніх позитивних особистих якостей.

Дітям властиві *наслідування й підвищене навіювання*, що має як позитивне, так і негативне значення для засвоєння норм і правил поведінки. У зв'язку з недостатнім розвитком самосвідомості та малим життєвим досвідом, діти можуть наслідувати небажані форми поведінки: грубість, недисциплінованість тощо. В інших випадках, коли вони беруть за взірць поведінку улюбленого вчителя, авторитетних для них дорослих, наслідування і підвищене навіювання полегшують засвоєння позитивних норм і правил поведінки. У цей період зростає роль особистого прикладу дорослих, передусім учителя.

Плануючи тренінг для дітей, які не знайомі між собою, крім вправ на знайомство, бажано передбачити вправи для створення групової атмосфери (дивись додаток). Ці вправи не є обов'язковими, але вони використовуються під час формування групи, коли учасники не знають один одного. На початку тренінгу діти, скоріше за все, будуть почуватися некомфортно, тому що їм необхідно адаптуватися в нових умовах. Беручи до уваги зазначені вище вікові особливості дітей, бажано звернути їхню увагу на приміщення, в якому проводиться тренінг і в якому вони будуть знаходитися певний проміжок часу. Такі вправи досить прості: учасник має можливість побувати у кожній частині приміщення, звернути увагу на всі елементи інтер'єру (які потім вже не будуть його відволікати) та адаптуватися у приміщенні. Після завершення такої вправи діти почуваються більш вільно, захисні механізми слабшають, знижується загальний рівень психологічної напруги.

З огляду на вікові особливості школярів та якщо дозволяє час, бажано провести вправу на розвиток емпатії (такі вправи ви знайдете у додатку). Діти можуть дивитися та начебто слухати тренера, але насправді не бачити і не чути його. Навчитися бачити та чути людину,

яка знаходиться поруч, – велике досягнення для дитини. Кожна така гра допомагає розвивати психологічну спостережливість та увагу, можливість відчувати настрій інших. Крім того, розвиток сенсорних можливостей та навичок рефлексії сприятиме формуванню необхідних компетенцій та навичок безпечної поведінки у мережі Інтернет.

У структурі тренінгу для дітей молодшого шкільного віку необхідно планувати вправи на концентрацію уваги. Дитина не може на тривалий час зосередити свою увагу на певній темі. Але за допомогою таких вправ тренер може досить легко та невимушено концентрувати увагу навколо теми Інтернету та його потенційних ризиків і небезпек. Важливо й те, що такі вправи не потребують глибокого аналізу та обговорення, і тому вони не напружують дітей.

Якщо є можливість виходу у мережу Інтернет, дуже корисною буде наочна демонстрація дітям її потужності як ресурсу інформації. Зайдіть на сайт «Онляндія» (www.onlandia.org.ua) в розділ для дітей 7-10 років (<http://www.onlandia.org.ua/ukr/pupils7-10.aspx>). Тут Ви матимете змогу наочно продемонструвати дітям можливості електронної пошти. Учасники тренінгу дізнаються про небезпеки, які можуть трапитися у випадку неправильного користування електронною поштою. Анімаційний сюжет одночасно дозволить зацікавити дітей темою безпеки в Інтернеті. Після завершення перегляду є можливість провести самоперевірку засвоєних знань. Дітям молодшого шкільного віку подобається така форма навчання, і вони залюбки долучаються до такої діяльності.

Логічним завершенням тренінгу буде створення із дітьми безпечної електронної скриньки на сайті «Онляндія». Зайдіть в розділ «Електронна пошта» та допоможіть дітям створити власну скриньку без вірусів, спаму та реклами.

5.2. Формування у дітей навичок критичного мислення

Практичний досвід формування у дітей стійкої мотивації до безпечної поведінки у мережі Інтернет свідчить про необхідність формування у дітей навичок *самостійного мислення*. Після завершення тренінгів діти поінформовані про ризики в Інтернеті. Але самі знання не є запорукою бажаного результату. Унікальність тренінгів, які пропонуються в даному посібнику, полягає в тому, що під час занять діти самостійно навчаються аналізувати ту інформацію, яку вони

отримують, подорожуючи віртуальним світом. Таким чином вони навчаються критично мислити.

Термін «критичне мислення» з першого погляду є досить розмитим та багатозначним. Він викликає численні асоціації та тлумачення. Для ясності подальшого викладу розглянемо одне прийнятне його роз'яснення.

Американський фахівець Річард Пауль у книзі з досить показовою назвою «Критичне мислення: що потрібно кожній людині, щоб вижити у швидкоплинному світі» запропонував таке визначення: критичне мислення – це мислення про мислення, коли ви мислите задля вдосконалення свого мислення. Тут є важливими дві обставини: 1) критичне мислення – це не просте мислення, а мислення, яке спричиняє самовдосконалення; 2) бажане самовдосконалення приходить з навичками використання стандартів коректної оцінки процесу мислення. Одним словом, це самовдосконалення мислення на підставі певних стандартів.

Професор *Девід Клустер* дає, на погляд *Дементієвської Н.П.*, найбільш зрозуміле і корисне для вчителів визначення критичного мислення. Він називає п'ять складових критичного мислення [1]:

1. *Критичне мислення – мислення самостійне.* Ніхто не може думати за нас. Ми формуємо свої ідеї, оцінки й переконання винятково самі і для самих себе. Для того, щоб сформувані власну думку про історичну особу, недостатньо знати біографію цієї історичної особистості, недостатньо розуміти значення її діяльності, висловлене тим або іншим істориком. Необхідно мати навички критичного мислення. Наші ж учні часто вважають, що достатньо сказати: «Я вважаю ...» або «На мою думку ...», щоб їх відповідь була самостійною. Мислити критично можна в будь-якому віці, навіть малята здатні думати критично і цілком самостійно. Самостійність – перша і, можливо, найважливіша ознака критичного мислення.

2. *Інформація є відправним, а не кінцевим пунктом критичного мислення.* Знання створює базу, без якої людина не може мислити критично. Щоб висловити складну думку, потрібно переосмислити велику кількість фактів, ідей, теорій, концепцій.

3. *Критичне мислення починається з постановки запитань і з'ясування проблем, які потрібно вирішити.* Люди допитливі за своєю природою. Ми помічаємо щось нове і хочемо довідатися, що

це таке. «Жити – означає мати проблеми, а вирішувати їх – означає зростати інтелектуально», - писав Дж. Гілфорд. Американський філософ і педагог Джон Дьюї вважав, що критичне мислення виникає тоді, коли учні починають працювати над вирішенням конкретної проблеми: «Тільки борючись із конкретною проблемою, відшукуючи власний вихід із ситуації, учень дійсно думає».

4. *Критичне мислення прагне до переконливої аргументації.* Критично мисляча людина може знайти власний спосіб розв'язання проблеми й обґрунтувати це рішення розумними доказами. Вона усвідомлює, що існують ще й інші шляхи розв'язання проблеми, але може довести, що її рішення є оптимальним. Будь-яка аргументація містить у собі чотири основних елементи:

- твердження (теза, основна ідея),
- доводи,
- докази (цифри, цитата з тексту, особливий досвід),
- підстава (точка відліку, що дає обґрунтування всієї аргументації).

5. *Критичне мислення є мислення соціальне.* Особиста думка перевіряється й удосконалюється, коли нею поділитися з іншими. Коли ми дискутуємо, сперечаємося, обмінюємося думками з іншими людьми, ми уточнюємо й поглиблюємо свою власну позицію. Тому з метою формування в учнів навичок критичного мислення необхідно використовувати інтерактивні методи: парну й групову роботу, дискусії й дебати, проекти й письмові роботи.

Основні техніки формування і розвитку в учнів критичного мислення

Основне завдання тренера, який навчає учнів мислити критично, – це навчити їх ставити запитання, формулювати проблеми та вирішувати їх, тому що вміння вирішувати проблеми – шлях до досягнення мети, шлях до успіху.

Умови для формування критичного мислення у школі:

- * сприятливий психологічний клімат та навчальний простір;
- * готовність вчителя до формування в учнів навичок критичного мислення;
- * знання основних понять, технік, методики;

* вміння ідентифікувати й оцінювати рівень розвитку критичного мислення у себе і своїх вихованців.

На наш погляд, дітей віком 7-11 років цілком достатньо озброїти знаннями наступних трьох параметрів оцінювання достовірності сайтів, що використовуються для навчальних цілей.

1. Навігація та зручність використання. Для того, щоб можна було скористатися корисною інформацією, розміщеною на сайті, важливо, щоб такий сайт можна було досить просто знайти та ефективно використовувати. Він має бути зручним у навігації, щоб у ньому, рухаючись по гіперпосиланнях, можна було легко знаходити потрібну інформацію, оминаючи зайву, нецікаву, непотрібну.

2. Авторство. На сайті має бути інформація як про власників (тих, хто створив і розмістив сайт в Інтернеті), так і про авторів статей, розміщених на ньому. На сайті мають бути такі відомості, як повне ім'я автора, рід його занять, його досягнення в певній галузі знань.

3. Надійність змісту. Учні мають з'ясувати: містить сайт тільки рекламу, чи власну точку зору автора, чи виключно наукові знання, і чи може насправді він бути джерелом інформації, необхідної для навчання? З якою метою надається чи пропонується інформація і кому вона вигідна, корисна? Дуже важливо, щоб учні усвідомлювали, чи потрібен їм цей сайт для вирішення навчального завдання.

5.3. Структурно-логічна модель тренінгу для дітей 7-10 років з безпеки в Інтернеті

1	Мета тренінгової програми	Формування у дітей стійкої мотивації до безпечної поведінки у мережі Інтернет
2	Перелік конкретних завдань тренінгової програми:	<ol style="list-style-type: none"> 1. Озброїти учасників знаннями про ризики в Інтернеті. 2. Сформувати в учасників розуміння необхідності дотримання правил безпечної поведінки в Інтернеті. 3. Сформувати навички користування правилами безпечної поведінки в Інтернеті.

		4. Ознайомити учасників тренінгу із ресурсами Інтернету: освітніми, інформаційними та розважальними.	
3	Цільова група – категорія учасників:	Діти віком 7-10 років	
4	Кількість учасників тренінгового заняття:	До 35	
5	Час, необхідний для проведення тренінгу:	1,5 години або 2 уроки по 45 хвилин	
6	Структура тренінгу		
	Вид діяльності	Опис діяльності	Тривалість
	Вступ	Тренер розповідає учасникам про програму «Онляндія - безпека дітей в Інтернеті», повідомляє тему та мету тренінгу	5 хв.
	Мотивація до діяльності	Вправа на формування в учасників мотивації до активної та плідної участі у тренінгу	
	Очікування	Вправа на визначення очікувань учасників тренінгу	
	Правила	Група під керівництвом тренера обговорює та приймає правила поведінки на тренінгу	5 хв.
	Знайомство	Вибір вправи з додатку. Лише у випадку, коли учасники не знайомі між собою.	5 хв.
	Інформативний блок №1.	Із використанням презентації PowerPoint тренер інформує про проникнення Інтернету в усі сфери життєдіяльності суспільства.	
	Групова діяльність	Обговорення корисності ресурсів Інтернету	

Групова діяльність	Учасники, об'єднавшись у 2 групи, готують по одній презентації «Ризики від Інтернет-ресурсів». Презентація групової діяльності. Узагальнення інформації тренером.	10 хв 5 хв.
Інформативний блок №2.	Із використанням презентації PowerPoint тренер інформує про небезпеки в мережі Інтернет.	10 хв.
Мозковий штурм	Тренер пропонує для обговорення проблемне запитання: «Як захистити себе в мережі Інтернет?». Обговорення.	5 хв.
Рухавка	Вправа на усвідомлення необхідності дотримання правил безпеки в Інтернеті.	5 хв.
Рухавка	Вправа на усвідомлення необхідності дотримання правил безпеки в соціальних мережах.	5 хв.
Групова діяльність	Учасники, об'єднавшись у 2 групи, готують по одній презентації: «Правила безпеки під час роботи в мережі Інтернет для моїх молодших (старших) братів (сестер) Презентація діяльності.	5 хв. 1 хв.
Узагальнення	Тренер узагальнює результати тренінгу.	5 хв.
Вправа на узагальнення	Вправа на узагальнення матеріалу (дивись додаток).	10 хв.

	Обладнання:	Тренінг проводиться у просторому приміщенні. Стільці розташовані по колу із достатнім для вправ простором посередині. Фліпчарт, маркери різнокольорові, папір А-4, проектор, ноутбук, стікери, кольоровий папір, клей, скотч.
	Оцінка тренінгу (критерії успіху):	Результати тренінгу можна відслідкувати за висловлюваннями учасників під час підбиття підсумків і презентації «Схема впровадження програми з безпеки дітей в Інтернеті в навчально-виховний процес».
	Додатки та роздатковий матеріал до тренінгу:	Сувенірна та поліграфічна продукція з символікою та інформацією «Онляндії».

6. Організація навчально-виховної роботи

з дітьми 11-18 років

6.1. Врахування психологічних особливостей дітей при організації тренінгів

Плануючи тренінг для учнів середнього та старшого шкільного віку, необхідно також враховувати особливості психічних процесів та вікові психологічні зміни, які відбуваються у цей бурхливий період розвитку.

1. Необхідно враховувати, що у підлітковому віці спостерігається збільшення обсягу уваги, підвищення стійкості уваги та розвиток здатності до переключення та розподілу уваги. Також у підлітків відмічається погіршення результатів навчальної діяльності. Це пояснюється тим, що розумові здібності підлітка, на відміну від здібностей молодшого школяра, набувають нової якості: вони стають опосередкованими. Це відбувається завдяки розвитку понятійного, мовно-логічного, абстрактного мислення. Підліток може оперувати поняттями, розмірковувати про властивості та якості предметів, висувати гіпотези, планувати дослідницьку діяльність і засвоювати

великі масиви інформації. Тому дуже доречним під час тренінгу буде оперування саме поняттями та категоріями, а не прикладами.

2. У підлітків з'являються нові інтереси, переживання та хронічна емоційна нестабільність, яка виявляється в імпульсивності, нестриманості, іноді агресивності. Тому треба бути готовим до можливого неприйняття тренера. У такому випадку краще обговорювати не ті теми, які заплановані, а теми, які цікавлять дітей: спілкування у соціальних мережах, знайомство у мережі Інтернет, он-лайн-придбання послуг та товарів тощо.

3. Розумова діяльність підлітка, як і його поведінка, залежить від стану його мотиваційної сфери. Підліток уважний тільки до того, що якимось пов'язано з його актуальними потребами та переживаннями. Його переживання тією чи іншою мірою пов'язані з пошуком себе, з пізнанням своїх здібностей та можливостей, з прагненням дізнатися, як оцінюють його оточуючі, з постійним перебиранням на себе різних дорослих ролей та гострою необхідністю у формуванні власного образу «Я». Це для підлітка головне. І якщо тренінг сприяє розвитку особистості, якщо навчальна ситуація пов'язана з актуальними переживаннями, якщо характер і форми спілкування з підлітком допомагають йому здобути більш дорослу позицію, то увага стає стійкою та концентрованою. Тому дуже результативним у плані формування стійкої мотивації до безпечної поведінки у мережі Інтернет є обговорення тем соціальних мереж, сайтів знайомств тощо. У цей час досить доречно обговорювати питання перегляду сайтів із дорослим контентом.

4. Учні-підлітки мають індивідуальні відмінності в характері мнемічної діяльності: якщо учні 5-го класу більше використовують зовнішні прийоми запам'ятовування (асоціації, смислове групування), то учні 8-го класу - більше опосередковані прийоми запам'ятовування та пошук специфічних прийомів для вивчення нового матеріалу. Центральне місце посідає аналіз змісту матеріалу, його своєрідності та внутрішньої логіки. Тому цей аспект враховується під час вибору ігрових методик та завдань.

5. У підлітковому віці при явних акцентуаціях особливості характеру загострюються, а завдяки впливу психогенних чинників можливі порушення адаптації, відхилення у поведінці. Підліток демонструє свій тип характеру в сім'ї та школі, під час навчання та

відпочинку, праці та розваг, у звичайних умовах або у складних ситуаціях. Завжди й усюди гіперактивний підліток надто енергійний, шизоїдний ховається від оточуючих, істероїдний намагається привернути до себе увагу інших. Тому необхідно бути готовим до таких проявів під час тренінгу. Найкращий шлях подолання проблеми – звернути увагу на підлітка та дати йому індивідуальне завдання.

Враховуючи вищезазначене, у структуру тренінгу бажано включити вправи на зняття тактильних бар'єрів. Особливо, коли учасники незнайомі між собою. Зняття тактильних бар'єрів у спілкування допомагає встановленню тактильного контакту, який сприяє згуртуванню групи, взаєморозумінню та підвищенню рівня довіри один до одного. Використовувати такі ігри бажано на першому занятті.

Обов'язково вводиться до структури тренінгу і вправа на підвищення рівня взаємодії у групі. Взаємодія – складний процес побудови стосунків між членами групи. І від того, наскільки вона буде ефективною, залежить, в більшості випадків, результативність самого тренінгу. Звісно, ми можемо поінформувати дітей про ризики у мережі Інтернет. Але не факт, що діти одразу будуть використовувати у власному житті отримані знання. Тому ми працюємо до досягнення результату – дотримання дітьми правил безпечної поведінки у мережі Інтернет.

Знаючи вікові особливості учасників, тренер може потрапити у ситуацію, коли група знаходиться у тому емоційному стані, який не сприяє майбутній діяльності під час тренінгу. У такому випадку радимо не змінювати емоційний стан учасників, а налаштувати дітей на ту діяльність, яка відповідає їхньому емоційному стану. Важливо підібрати вправу на регуляцію психологічного або емоційного стану, яка не лише буде адекватною цілям тренінгу, а й згуртує учасників, налаштує на роботу. Подібні вправи бажано проводити не лише на початку тренінгу, але й у тих випадках, коли завершується смисловий блок (модуль) тренінгу.

Досить часто у нагоді стають вправи, спрямовані на зняття агресії. Вони допомагають вирішити проблему регуляції емоційного стану учасників і одночасно сприяють вдалому досягненню мети тренінгу. Тренери часто запитують: яка ж причина агресивної поведінки групи? Одряду необхідно відзначити, що виникнення емоційної напруги (агресії) є природною особливістю групової динаміки. Якщо групова енергія виробляється активніше, ніж витрачається, то вона, звісно,

трансформується у напругу. Такої агресії досить легко уникнути, якщо створювати умови для максимальної активності учасників. Не слід забувати і про вікові особливості дітей.

6.2. Використання навичок критичного мислення при оцінюванні Інтернет-ресурсів

Якщо є можливість провести декілька тренінгів із теми безпеки дітей в Інтернеті, то ми радимо використовувати методи оцінювання Web-сайтів за методикою *Дементієвської Н.П.*: за формальними критеріями та мисленневими операціями. Спочатку учням пропонується провести оцінку Web-ресурсу за формальними індикаторами, а потім застосувати навички критичного мислення.

Формальні критерії (індикатори) оцінювання сайтів (їх можна просто і легко виявити на сайті):

а) надійність джерела та/або автора Web-документа. Чим надійніше джерело (автор) статті чи авторитетніша назва організації, тим більше довіри до них в Інтернеті, тим цінніша Web-сторінка. Учням можна пояснити різницю між авторами статей та власниками сайтів. Важливо, щоб учні могли встановити: людині, групі людей чи організації належить той чи інший сайт. Додатковою ознакою надійності джерела є забезпечення на сторінці так званого «зворотнього зв'язку» з автором, тобто наявність електронної адреси чи організація форуму (відстроченого спілкування) або навіть чату з автором (авторами) Web-документа. Сприяє довірі до сайту і наявність інформації про рівень кваліфікації автора, його заслуги в певній галузі знань – це є підтвердженням того, що він може бути експертом з цього питання;

б) основні ознаки надійності URL-адреси Web-сайту. Учні мають вміння визначати URL-адресу сайту і звертати особливу увагу на деякі елементи адреси. Їх потрібно навчити базовим знанням про формування доменних імен, які надаються сайтам. Зокрема, вони мають знати про певну комбінацію літер у кінці доменного імені, наприклад :

* .gov – це вказує на те, що це сайт державної установи,

- * .edu – це ознака освітніх установ, університетів,
- * .com – використовується для комерційних організацій, які створені для отримання прибутку,
- * .org – в основному, ознака неприбуткових організацій;

в) наявність дати створення сайту, дат розміщення матеріалів та оновлення сайту. Сайт має періодично оновлюватися, щоб розміщена на ньому інформація була достовірною, свіжою та точною. Це свідчить про те, що автори піклуються про висвітлення поточних подій, слідкують за тим, що відбувається у світі, в тому числі і в галузі науки. Це стосується, в першу чергу, сайтів, які пов'язані з висвітленням щоденних подій та з наукою. Учням треба показати, що відомості про створення та оновлення сайту зазвичай розміщені в нижній частині сторінки.

г) наявність у статті слів узагальнюючого (всі, завжди, ніколи, ніхто, всім відомо, тощо) та оціночного змісту (хороші, погані, найкращі, здорові, шкідливі тощо) є індикатором ідентифікації наукових та науково-популярних статей, оскільки такі слова не притаманні мові науковців та їхнім висновкам. У наукових та науково-популярних статтях справжні незаангажовані вчені завжди показують переваги певної ідеї, методу, виробу, продукту, висвітлюють їхні недоліки та застереження щодо застосування;

д) наявність граматичних та орфографічних помилок на сайті, фактичних помилок в інформації. Учні повинні вміти оцінювати загальний вигляд сайту та помічати помилки. На сайтах, які створюються вченими і освіченими людьми, практично немає таких помилок. Крім того, сайт повинен легко завантажуватися, фон та шрифт сайту мають бути такими, щоб його можна було легко читати, - це також свідчить про загальну культуру та освіченість тих, хто публікує інформацію.

Як проаналізувати сайти?

(Які необхідні для цього мисленнєві операції, навички критичного мислення - навички мислення високого рівня, когнітивні знання - знання про закономірності мислення людей та про власне мислення).

1. З'ясування причин, через які автор сайту публікує свою інформацію. Дуже важливо визначати головне призначення сайтів, цілі їх створення і розміщення в Інтернеті. Мета сайту може бути завуальованою, можна і потрібно навчати учнів визначати такі неявні, а іноді й приховані цілі авторів. Учні, переглядаючи сайти, мають ставити собі запитання: *Що цей сайт намагається повідомити? З якою метою він був створений: продавати певні вироби, пропагувати ідеї чи пропонувати розваги?*

2. Виявлення перекрученої, «викривленої» логіки; порушень логіки, аргументації. Важливо навчити учнів логічно мислити, доводити тези, висловлювати та перевіряти гіпотези, знаходити аргументи, виявляти взаємозв'язок причин та наслідків.

3. Виявлення фактів та їх інтерпретація. Важливо навчити учнів знаходити аргументацію в тексті статті та визначати, що серед аргументів є фактом, а що - власною думкою автора.

4. Виявлення статей з прихованою пропагандою, рекламою. Найпоширенішим засобом в Інтернеті є прихована реклама, чи реклама, яка «маскується» під наукові або інформаційні статті.

Під час тренінгу логічним буде використання сучасних ІКТ. Запропонуйте дітям переглянути цікаві анімаційні матеріали на сайті «Онляндія» www.onlandia.org.ua в розділі для дітей 11-14 років (<http://www.onlandia.org.ua/ukr/mail.aspx>). Це реальні історії, які вчать правилам безпеки під час користування електронною скринькою, спілкування в чатах та інших програмах обміну миттєвими повідомленнями, соціальних мережах тощо. Дорослі для дітей старшого віку не завжди є авторитетами, тому дозвольте Інтернету повчати дітей.

6.3. Структурно-логічна модель тренінгу для дітей 11-18 років з безпеки в Інтернеті

1	Мета тренінгової програми	Формування у дітей стійкої мотивації до безпечної поведінки у мережі Інтернет	
2	Перелік конкретних завдань тренінгової програми:	<ol style="list-style-type: none"> 1. Озброїти учасників знаннями про ризики в Інтернеті. 2. Сформувати в учасників розуміння необхідності дотримання правил безпечної поведінки в Інтернеті. 3. Сформувати навички користування правилами безпечної поведінки в Інтернеті. 4. Ознайомити учасників тренінгу із ресурсами Інтернету: освітніми, інформаційними та розважальними. 	
3	Цільова група – категорія учасників:	Діти віком 7-10 років	
4	Кількість учасників тренінгового заняття:	До 35	
5	Час, необхідний для проведення тренінгу:	1,5 години або 2 уроки по 45 хвилин	
6	Структура тренінгу		
	Вид діяльності	Опис діяльності	Тривалість
	Вступ	Тренер розповідає учасникам про програму «Онляндія - безпека дітей в Інтернеті», повідомляє тему та мету тренінгу	5 хв.
	Мотивація до діяльності	Вправа на формування в учасників мотивації до активної та плідної участі у тренінгу	
	Очікування	Вправа на визначення очікувань учасників тренінгу	
	Правила	Група під керівництвом тренера обговорює та приймає	5 хв.

	правила поведінки на тренінгу.	5 хв.
Знайомство	Вибір вправи з додатку. Лише у випадку, коли учасники не знайомі між собою.	5 хв.
Інформативний блок №1.	Із використанням презентації PowerPoint тренер інформує про проникнення Інтернету в усі сфери життєдіяльності суспільства.	5 хв.
Групова діяльність	Обговорення корисності ресурсів Інтернету.	5 хв.
Групова діяльність	Учасники, об'єднавшись у 2 групи, готують по одній презентації «Ризики від Інтернет-ресурсів».	10 хв.
Групова діяльність	Презентація групової діяльності. Узагальнення інформації тренером.	5 хв.
Інформативний блок №2.	Із використанням презентації PowerPoint тренер інформує про небезпеки в мережі Інтернет.	10 хв.
Мозковий штурм	Тренер пропонує для обговорення проблемне запитання: «Як захистити себе в мережі Інтернет?». Обговорення.	5 хв.
Рухавка	Вправа на усвідомлення необхідності дотримання правил безпеки в Інтернеті.	5 хв.
Рухавка	Вправа на формування стійкої мотивації до безпечної поведінки у мережі Інтернет: - під час спілкування у соціальних мережах; - під час обміну миттєвими повідомленнями;	10 хв.

	<ul style="list-style-type: none"> - під час обміну фотографіями та іншою особистою інформацією; - під час користування Інтернет-магазинами; - при користуванні електронною поштою; - при потраплянні на сайти із дорослим контентом та контентом, який є небажаним для дітей. 	
Групова діяльність	<p>Учасники, об'єднавшись у 2 групи, готують по одній презентації: «Правила безпеки під час роботи в мережі Інтернет для моїх молодших (старших) братів (сестер).</p> <p>Презентація діяльності.</p>	<p>10 хв.</p> <p>10 хв.</p>
Узагальнення	Тренер узагальнює результати тренінгу.	5 хв.
Вправа на узагальнення	Вправа на узагальнення матеріалу (дивись додаток).	10 хв.
Обладнання:	Тренінг проводиться у просторому приміщенні. Стільці розташовані по колу із достатнім для вправ простором посередині. Фліпчарт, маркери різнокольорові, папір А-4, проектор, ноутбук, стікери, кольоровий папір, клей, скотч.	
Оцінка тренінгу (критерії успіху):	Результати тренінгу можна відслідкувати за висловлюваннями учасників під час підбиття підсумків і презентації «Схема впровадження програми з безпеки дітей в Інтернеті в навчально-виховний процес».	
Додатки та роздатковий матеріал до тренінгу:	Сувенірна та поліграфічна продукція з символікою та інформацією «Онляндії».	

РОЗДІЛ IV. ВІДПОВІДАЛЬНІСТЬ БАТЬКІВ ЗА БЕЗПЕКУ ДІТЕЙ В ІНТЕРНЕТІ. РЕКОМЕНДАЦІЇ ДЛЯ ПЕДАГОГІВ З ПИТАНЬ ОРГАНІЗАЦІЇ ПРЕВЕНТИВНОЇ РОБОТИ З БАТЬКАМИ

Психологічні особливості дорослої людини досить широко варіюють у вікових межах: психологічні риси і погляди 35-річних та 45-річних батьків можуть докорінно відрізнятись. Але всіх батьків об'єднує одна особливість: кожен дбає про безпеку своєї дитини, у тому числі і під час перебування у мережі Інтернет.

Інтернет відкриває дітям і молоді фантастичні можливості для дослідження, зв'язку та творчості в он-лайн. Однак із використанням Інтернету пов'язані певні ризики. Зокрема, Інтернет — це вікно у світ також і для дорослих, і він містить матеріали, що не підходять для дітей.

Як батьки можуть допомогти дітям мінімізувати ризики? На це питання немає однозначної відповіді, адже ризики варіюють в залежності від віку та рівня комп'ютерної грамотності дитини.

Як це не дивно, але більшість українських батьків, на жаль, не до кінця усвідомлюють загрози, на які може натрапити їхня дитина в мережі Інтернет. Так, наприкінці 2009 року Інститутом соціології НАН України було проведено дослідження, згідно з яким, за оцінкою дітей, батьки лише у 24% випадків запитують, які саме сайти вони відвідують у мобільному Інтернеті. Відвідуваннями стаціонарного Інтернету цікавляться в 57% випадків. Але лише 5% батьків цікавляться більш детально змістом сайтів, які діти відвідують у мобільному Інтернеті, та 30% — у стаціонарному.

За нашими даними, більшість батьків вважає, що, придбавши комп'ютер та підключивши його до мережі Інтернет, можна позбутися багатьох проблем. Адже, на думку батьків, дитина більше часу перебуває вдома, під наглядом, нагодована та доглянута; які можуть бути загрози? Якої шкоди можуть завдати віртуальні друзі?

Саме тому ми рекомендуємо впроваджувати програму з безпеки дітей в Інтернеті комплексно. Окремі тренінги для дітей не принесуть бажаних результатів. Потрібна комплексна програма, спрямована на інформування вчителів, дітей та їхніх батьків. Для батьків ми радимо проводити тематичні батьківські збори. Враховуючи досвід організації та проведення таких зборів, ми можемо констатувати, що 98% батьків

із подивом дізнаються про ті реальні загрози, на які можуть натрапити їхні діти, мандруючи віртуальним світом, і починають говорити про необхідність запровадження у навчальному закладі курсу з безпеки в Інтернеті як для дітей, так і для батьків.

Превентивну роботу з батьками ми розподіляємо на наступні тематичні **модулі**.

1. Захист власного комп'ютера.
2. Захист дитини в он-лайні.
3. Дотримання правил безпечного користування Інтернетом.

Захист комп'ютера. На сьогодні існує досить багато різноманітних ресурсів, які дозволяють максимально захистити комп'ютер від злому та інших небажаних дій. Узагальнюючи всі поради, ми радимо батькам:

- періодично оновлювати операційну систему;
- використовувати антивірусну програму. Ми радимо встановити безкоштовну антивірусну програму *Microsoft Security Essentials*, яка захищає комп'ютер у реальному часі. Більше про антивіруси можна дізнатися на Web-сторінці сайту Microsoft http://www.microsoft.com/security_essentials;

- використовувати брандмауер;
- робити резервні копії важливих файлів;
- бути обережними, завантажуючи вміст.

На батьківських зборах немає необхідності проводити детальне навчання комп'ютерній грамотності. Достатньо лише розповісти про корисні ресурси та надати можливість самостійно знайти їх у мережі Інтернет. Так, наприклад, рекомендуємо лише повідомити батькам, що система батьківського контролю Windows 7 додасть душевного спокою та впевненості у тому, що вони можуть керувати діями дітей, які ті виконують на персональному комп'ютері. Тут можна навіть вказати, в які ігри можуть грати діти на комп'ютері та які програми використовувати. Можна зазначити час, коли дитині дозволено користуватися комп'ютером.

Безпека сім'ї Windows Live — це безкоштовний засіб, який можна завантажити для Windows 7. Він дає змогу керувати діями дітей в Інтернеті та відстежувати їхню діяльність. Web-фільтрація та керування контактами, наприклад, допоможуть визначити коло осіб, з якими діти можуть спілкуватися за допомогою служб Windows Live Hotmail, Messenger і Spaces. Установивши параметри для кожної дитини,

можна навіть отримати звіт про її діяльність, в якому зазначається, як саме вона використовувала комп'ютер і які Web-сайти відвідувала. А завдяки можливості віддаленого перегляду звітів і зміни параметрів можна стежити за діями своїх дітей з будь-якого місцезнаходження та відстані.

Багато корисного про безпеку користування Інтернетом батьки можуть дізнатися, відвідавши сайт «Онляндія». У розділі для батьків дорослі можуть пройти безкоштовне он-лайн-навчання, як налаштувати власний комп'ютер на максимально безпечне використання. Невелика конкретна інформація і поради, що стосуються сучасних мультимедійних технологій, будуть корисними для дорослої людини.

Захист дитини в он-лайні.

Ключовими порадами, які допоможуть батькам захистити дитину від Інтернет-шахраїв, мають бути наступні:

- будьте обережні, надаючи в Інтернеті свою особисту інформацію;
- думайте про те, з ким ви розмовляєте;
- пам'ятайте, що в Інтернеті не всі джерела є надійними і не всі люди чесними.

Дотримання правил безпечного користування Інтернетом

Маючи певний досвід тренінгової діяльності з батьками щодо безпеки дітей в Інтернеті, ми узагальнили ці поради і сформулювали у вигляді 6 правил для батьків. Ці правила розташовані на сайті «Онляндія» у розділі для батьків http://www.onlandia.org.ua/ukr/v_turvallisesti_6rules.aspx

1. Розмістіть комп'ютер у кімнаті, яку використовують усі члени родини.

Іноді діти тримають у секреті те, що вони користуються Інтернетом. Вони можуть не бажати того, аби батьки знали про їхнє спілкування та дії в мережі. Не потрібно на це занадто емоційно реагувати, а треба зробити все можливе, щоб зняти психологічну напругу та відновити довіру у стосунках з дитиною. Обговорювати можливі труднощі чи небезпеки, що виникають під час користування Інтернетом, легше, коли комп'ютер знаходиться у спільній кімнаті. Крім того, ви можете використовувати Інтернет разом із дитиною. Таким чином, розмови про Інтернет та контроль за його використанням стануть повсякденною частиною вашого родинного життя.

2. Використовуйте будильник для обмеження часу, який дитина проводить в Інтернеті. Заздалегідь погодьте тривалість перебування в Інтернеті.

Бажано визначити, який час дитина може перебувати в он-лайні, аби не нанести шкоди стану її здоров'я та не сприяти комп'ютерній залежності, яка стала великою проблемою у всьому світі.

Обговоріть час перебування дитини в Інтернеті та домовтеся про використання будильника. Таким чином ви уникнете можливих конфліктних ситуацій.

3. Використовуйте технічні засоби захисту: функції батьківського контролю в операційній системі, антивірус та спам-фільтр.

Щоб користуватися комп'ютером, необов'язково знати всі його функціональні можливості. Запросіть спеціаліста, який налаштує операційну систему вашого комп'ютера та покаже, як працювати із батьківським контролем. Краще один раз побачити, аніж багато разів почути. Не використовуйте у себе вдома технічно незахищений комп'ютер.

Ви можете пройти он-лайн-навчання з метою ефективного використання функцій безпеки браузера та самостійно налаштувати батьківський контроль.

Встановіть Microsoft Security Essentials, і ваш комп'ютер буде захищеним у реальному часі від вірусів, програм-шпигунів та інших зловмисних програм.

4. Створіть сімейні правила он-лайн-безпеки для дітей.

Діти навчаються шляхом експериментування. Якщо ви зацікавлені у тому, аби ваша дитина навчалася не на своїх власних помилках, якомога частіше обговорюйте теми, пов'язані із Інтернетом. Ви можете розказати, наприклад, про достовірність інформації, розміщеної у мережі. Так ви невимушено створите свої сімейні правила Інтернет-безпеки. Традиції, норми та правила, які закріпилися у родині, довговічні.

5. Проводьте більше часу з дитиною, заохочуйте її до обговорення тем, пов'язаних з Інтернетом.

У кожного в житті трапляються помилки. Непотрібно сприймати помилки дітей як життєву проблему. Будуйте з дитиною довірливі стосунки задля того, аби бути впевненими, що у будь-якій ситуації вона

звернуться за допомогою саме до вас. Щоб не сталося, ваша дитина повинна знати, що вона завжди може розраховувати на ваше розуміння та підтримку. Хороший рецепт побудови довірливих відносин — щоденне спілкування та спільне проведення вільного часу. У невимушеній атмосфері набагато легше обговорювати «складні» питання.

6. Навчайте дітей критично ставитися до інформації в Інтернеті і не повідомляти конфіденційні дані в он-лайн.

Розкажіть дитині, що практично кожен може створити свій сайт, і при цьому ніхто не може проконтролювати достовірність інформації, розміщеної на такому сайті. Навчіть дитину використовувати інформацію з різних, але перевірених джерел.

На основі структурно-логічних моделей тренінгів, що були запропоновані в даному посібнику, можна розробити план власного тренінгу.

План тренінгу з безпеки в Інтернеті

Розробіть план власного тренінгу

1	Мета тренінгової програми	
2	Перелік конкретних завдань тренінгової програми:	
3	Цільова група – категорія учасників:	

4	Кількість учасників тренінгового заняття:		
5	Час, необхідний для проведення тренінгу:		
6	Структура тренінгу		
	Вид діяльності	Опис діяльності	Тривалість
	Вступ		
	Мотивація до діяльності		
	Очікування		

	Інформативний блок, інтерактивні вправи		
	Узагальнення		
	Обладнання:		
	Оцінка тренінгу (критерії успіху):		
	Додатки та роздатковий матеріал до тренінгу:		

Додаткові матеріали для організації та проведення тренінгів

Вправи на знайомство учасників

1. Вітання без слів

Учасникам пропонується протягом 2-3 хвилин вільно рухатися у приміщенні та привітати за цей час якомога більше людей. Робити це треба мовчки, без слів: кивком голови, рукостисканням, обіймами тощо. При цьому учасник має право використати кожен спосіб привітання лише один раз; для наступного привітання необхідно вигадати новий спосіб.

Психологічний сенс.

Зняття психологічної напруги, вільне спілкування.

Обговорення.

Кому скількох людей вдалося привітати? Що складніше: вигадати нові способи привітання чи їх продемонструвати? Можливо, хтось відчув психологічний дискомфорт? На якому етапі це відбулося?

Аналогія з Інтернетом.

Спілкуючись в Інтернеті, люди використовують допоміжні слова, символи, смайлики. Кожен вкладає в них своє значення, яке може бути незрозумілим для інших учасників.

2. Рухавка

Учасник, котрий починає вправу, називає групі власне ім'я та робить певний жест чи рух, яким виражає свій емоційний стан. Його сусід справа повторює ім'я та рухи попереднього учасника, після чого називає своє ім'я та демонструє свій рух. Третій учасник повторює імена і рухи двох попередніх учасників, після чого додає свої і т.д.

Психологічний сенс.

Знайомство, спілкування.

Обговорення.

Які емоції виникли у вас під час виконання вправи? Які рухи найбільше запам'яталися? Чому?

Аналогія з Інтернетом.

Спілкуючись в Інтернеті, люди використовують іноді зовсім незвичні форми спілкування. Яку інформацію можна отримати, спостерігаючи за тим, як люди себе презентують в Інтернеті?

3. Збери привітання

Учасникам протягом 30 секунд пропонується потиснути руки якомога більшої кількості учасників. Кожному учаснику можна тиснути руку лише один раз. Вправа має сенс, коли у групі більше 15 учасників.

Психологічний сенс.

Розминка.

Обговорення.

Кому скількох людей вдалося привітати? Можливо, хтось відчув психологічний дискомфорт? На яких етапах це відбувалося?

Аналогія з Інтернетом.

Досить часто співрозмовника в Інтернеті ми знаємо лише за його Ніком. Яку інформацію можна отримати про співрозмовника за його Ніком? Наприклад, людина, яка використовує Нік «лагідний», насправді може не бути лагідною.

4. Розшифруй своє ім'я

Учасникам пропонується записати своє ім'я і підібрати на кожну літеру слово, яке характеризує учасника. На роздуми відводиться 4-5 хвилин. Вправа досить складна і, можливо, не всі учасники матимуть змогу придумати риси характеру на всі літери імені. Достатньо розшифрувати 3-4 літери. Потім кожен учасник називає своє ім'я та ті характеристики, які йому вдалося придумати.

Наприклад, як можна розшифрувати ім'я Антон:

А — Активний

Н — Незалежний

Т — Тихий

О — Охайний

Н — Ніжний.

Психологічний сенс.

Можливість самопрезентації.

Обговорення.

Хто має бажання додати свої характеристики, які вам підходять, але їх назви не починаються з літер, з яких складається ваше ім'я?

Аналогія з Інтернетом.

Досить часто в соціальних мережах або інших ресурсах Інтернету користувачі змушені для отримання інформації або послуги приймати умови адміністратора. Ці умови бувають іноді ризиковані для самих користувачів, наприклад, повідомлення особистої інформації.

5. Вітер дме

Учасники знаходяться у колі. Ведучий говорить: «Вітер дме на того, у кого...» і називає ознаки деяких учасників. Це можуть бути деталі одягу, особливості їхньої зовнішності, психологічні якості, звички тощо. Учасники, які мають ці ознаки, повинні швидко помінятися місцями. Той, хто затримався, стає ведучим.

Психологічний сенс.

Вправа підкреслює відмінності учасників, дає можливість більше дізнатися один про одного, сприяє мобілізації уваги.

Обговорення.

Учасники обмінюються своїми емоціями, новими враженнями один про одного.

6. Візитівка

Кожен учасник із паперу форматом А-4 руками вириває будь-яку фігурку, яка символізує його ім'я, вік, мрії, бажання або нахили. Це може бути що завгодно: літера, цифра, яблуко, машина тощо.

На цій фігурці учасники пишуть своє ім'я.

Завдання. Познайомитися із якомога більшою кількістю учасників і дізнатися, що саме символізує його фігурка.

Обговорення.

Учасники обмінюються своїми враженнями, діляться інформацією, яку отримали про інших учасників.

Вправи на формування мотивації до діяльності

1. Асоціації

Тренер дає завдання учасникам: вони мають промовити будь-яке слово, а завдання їхнього сусіда зліва – швидко назвати перше слово-асоціацію, яке прийшло йому на думку.

Його сусід зліва промовляє свою асоціацію на його слово – і так по порядку.

У фіналі голосно промовляється останнє слово.

Звісно, перше слово і останнє – це зовсім різні слова.

Обговорення.

Учасники обмінюються своїми емоціями.

Аналогія з мережею Інтернет.

Це стосується і достовірності інформації у мережі Інтернет.

2. Ладоньки

Учасники об'єднуються у дві групи. Одна група утворює внутрішнє коло, друга – зовнішнє. Учасники розташовуються один навпроти іншого так, щоб у кожного була пара.

На першому етапі завдання всі учасники одночасно та ритмічно грають у всім відому гру «Ладоньки»: 1 – плеск у долоні, 2 – дві долоні паралельно плескають об долоні партнера, 3 – плеск у долоні, 4 – права рука піднімається догори, 5 – плеск у долоні, 6 – ліва рука піднімається догори, 7-8 – зовнішнє коло робить крок вправо, і партнери змінюються. Гра триває у тому ж самому ритмі без зупинок до тих пір, доки всі учасники не повернуться на свої місця.

Обговорення.

Учасники обмінюються своїми емоціями.

Аналогія з мережею Інтернет.

Інтернет – швидкий та потужний ресурс, який досить важко «наздогнати». Крім того, ця вправа яскраво демонструє, що лише завдяки командній діяльності можна досягти результату – не програти.

3. Я їду...

Вправа нагадує ситуацію, коли ми зі своїми друзями спізнувалися на заняття, забігали до громадського транспорту та займали вільні

місця: «Я тут сиджу!». До вас підсідає інший і говорить: «А я з тобою!»...

Учасники сидять у колі. Один стілець вільний.

Перший учасник пересідає на вільний стілець і промовляє: «А я їду!», наступний за ним пересаджується на звільнений стілець і говорить: «А я – засець!», третій: «А я – поряд», четвертий: «А я – з ...» і називає ім'я будь-кого з учасників, наприклад, «Іваном». Іван стрімко піднімається зі свого стільця і сідає на звільнений стілець.

Учасник зліва, який опинився поруч із звільненим стільцем Івана, сідає на нього і говорить: «А я їду!», і гра триває далі.

Важливо підтримувати швидкий темп гри. Для цього можна дати можливість учасникам 1-2 рази спробувати.

Ця вправа допомагає сформувати в учасників мотивацію до активної діяльності.

Обговорення.

Учасники обмінюються своїми емоціями.

Аналогія з мережею Інтернет.

Інтернет – постійний хаос, з яким дуже складно впоратися. Але, зрозумівши правила, можна легко орієнтуватися у цьому хаосі.

Вправи на розвиток емпатії

1. Б.З.Д.М.О.У.

Досить загадкова вправа, яка розшифровується досить легко: «Баскетболіст забив два м'ячі одним ударом». Вправа нагадує дитячу гру «Зіпсований телефон». Але, на відміну від останньої, вимагає точної фіксації на папері того, що зрозумів кожен учасник, спостерігаючи за жестикуляцією іншого учасника. Ця вправа дозволяє дізнатися тренеру про психологічні особливості кожного учасника. Вправа подобається і дітям, і дорослим.

Декілька учасників (7-8) виходять за двері.

Першому учаснику тренер говорить фразу: «Баскетболіст забив два м'ячі одним ударом».

Заходить один учасник. Перший за допомогою жестів передає йому цю фразу, яку той повинен записати на папері так, як він її зрозумів. Потім він показує жестама те, що сам зрозумів і записав на папері, і так далі.

У фіналі зачитуються всі фрази, починаючи від останньої і закінчуючи найпершою.

Обговорення.

Учасники обмінюються своїми емоціями. Після цього тренер пропонує відповісти на декілька запитань:

- Чи вдалося вам зберегти перший варіант ? Чому?
- Що Вам допомагало?
- Що вам заважало?

2. Гава

Вправа налаштовує учасників на необхідність прислухатися та придивитися до інших учасників.

Тренер показує учасникам будь-який предмет, наприклад, олівець, та просить всіх вийти на 1 хвилину з кімнати.

Залишившись наодинці, тренер кладе олівець в те місце, звідки його можна побачити, але треба бути при цьому дуже уважним: горщик із квіткою, карниз, між ніжками стола.

Тренер запрошує всіх зайти та знайти олівець.

Учасник, який знайшов олівець (побачив його), повинен одразу сісти.

Ця вправа, незважаючи на її простоту, дозволяє сконцентрувати увагу, а також виокремити одиничне із загального. Тренер не випадково спочатку показує предмет, а потім його ховає так, що лише уважний може його побачити.

Обговорення.

Учасники обмінюються своїми емоціями.

Аналізуючи вправу, тренер ставить запитання:

- На що ви орієнтувалися, коли виконували завдання?
- Що допомагало вам знайти предмет?
- Що заважало вам знайти предмет?

Вправи на концентрацію уваги

1. Друкована машинка

Учасники шикуються в одну лінію.

Тренер озвучує рядок із вірша, який необхідно «надрукувати».

Наприклад:

*В неволі, в самоті немає,
Нема з ким серце поєднати.
То сам собі оце шукаю
Когось, аби порозмовляти.*

Учасники називають по одній літері: 1-й – В, пропуск – всі плескають у долоні, 2-й – Н, 3-й – Е, 4-й – В і так далі.

Перехід до наступного рядка – всі тупають ногою.

Якщо учасник помиляється, то він вибуває з гри, а всі решта починають спочатку.

Ця вправа не потребує глибокого психологічного аналізу та обговорення після її закінчення, але вона дуже важлива та ефективна для концентрації уваги учасників.

Аналогія з Інтернетом.

Мережа Інтернет – швидкий віртуальний світ, в якому постійно треба мати концентровану увагу, щоб не потрапити у халепу.

2. Муха

Тренер на ватмані форматом А-1 креслить звичайний квадрат 5 x 5.

Посередині ставить «Х» - це і є «муха».

		X		

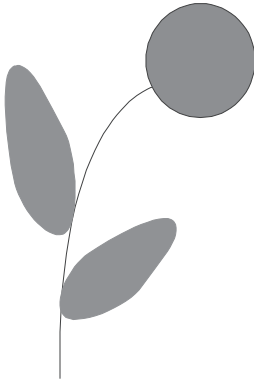
«Муха» за один хід може переміститися на 1 клітинку вгору або вниз, вліво або вправо. По діагоналі рухатися вона не може.

Потім учасники по колу починають «рухати» «муху» - по черзі називають її маршрут: вгору, вниз, вліво, вправо. Особливість вправи полягає в тому, що тренер не малює на ватмані рух «мухи» - учасники самостійно «рухають» її. «Муха» не може «вилетіти» за межі квадрата. Тренер слідкує за цим. Також не можна повертати «муху» зворотнім шляхом: якщо один учасник каже «вгору», то наступний не може її пересунути вниз.

У фіналі залишається один або декілька найуважніших учасників.

Вправа на визначення очікувань учасників

Квітка



Тренер заздалегідь готує ватман А-1 із зображенням квітки, але без пелюсток.

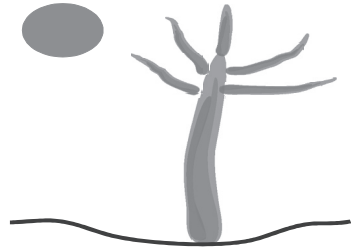
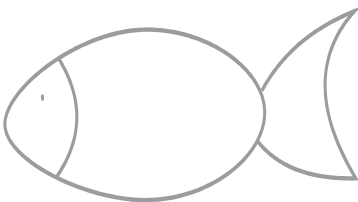
Учасникам роздаються різнокольорові стікери, на яких вони пишуть свої очікування.

Потім учасники по черзі підходять до квітки, голосно озвучують свої очікування (або не озвучують, в залежності від рівня згуртованості учасників тренінгу) та наклеюють свій стікер.

Таким чином квітка «обростає» яскравими пелюстками.

Як варіант, це може бути «риба»; стікери із очікуваннями наклеюються у вигляді луски.

Також це може бути і «посів» у вигляді «насінин» своїх очікувань. У такому варіанті цей ватман дуже знадобиться наприкінці тренінгу під час підбиття підсумків, коли учасники матимуть змогу одразу «повісити» плоди на дерево «результату тренінгу». Таким чином, очікування учасників та результати будуть наочно демонструвати ефективність тренінгу.



Вправа на формування мотивації до дотримання певних правил поведінки в Інтернеті

Кубик

Тренер до початку тренінгу готує 7 аркушів паперу форматом А-4, на яких пише великі цифри від 1 до 7. Ці аркуші тренер розклеює в різних кутках кімнати, але так, щоб усі учасники мали змогу їх

побачити. Не можна розмішувати цифри у порядку їх лічби: 1 не може бути поруч із 2.

Тренер декілька разів наголошує на тому, що зараз учасники візьмуть участь у грі.

Тренер повідомляє, що для кожного із учасників він мав підготувати сувенірну продукцію, але виявилось, що їх на тренінг з'явилося більше, ніж тренер планував, і тому деякі учасники мусять залишитися без подарунків. Але все повинно бути по-чесному, і тому зараз треба буде вирішити, хто ж саме додому піде без подарунка.

Учасникам пропонується обрати будь-яку цифру, яка, на їхню думку, буде щасливою для них.

Під час гри суворо забороняється розмовляти та підказувати один одному: кожен грає мовчки.

Після того, як учасники обрали свої цифри, тренер ще раз наголошує на тому, що під час гри не можна розмовляти, і дістає кубик. Тренер говорить, що за допомогою кубика він і обере ту групу, яка не отримає сьогодні подарунка.

Тренер підкидає кубик і підходить до групи, яка обрала ту цифру, що випала на кубіку.

Тренер звертається лише до членів цієї групи: «Які ваші враження?», «Як ви гадаєте, що зараз думають інші учасники тренінгу?». Потім тренер каже, що це була репетиція, і тому учасники цієї команди мають можливість змінити цифру. Після цього тренер пропонує змінити цифру всім учасникам, які мають таке бажання. Коли вибір зроблено, тренер знову підкидає кубик і звертається до команди, цифра якої випала на кубіку: «Які ваші враження?», «Як ви гадаєте, що зараз думають інші учасники тренінгу?». Тренер повідомляє гарну новину: це була ще одна спроба, і учасники ще раз можуть змінити цифру.

Гра триває до тих пір, доки тренер не помітить, що учасники під цифрою «7» не змінюють свого місця. І не даремно – на кубіку немає цифри 7! У цей момент тренер перериває гру і звертається до учасників, що обрали цифри «2», «3», «5»: «Що ви відчували кожного разу, коли я підкидав кубик?» Учасники зазвичай будуть казати, що хвилювалися. Потім тренер звертається до учасників під цифрою «7» з тим самим запитанням. Але учасники, які обрали цю цифру, скажуть, що не турбувалися про те, яка цифра випаде на кубіку, бо цифри 7 там немає!

Сенс гри полягає в тому, щоб учасники якомога швидше усвідомили правила цієї гри і перейшли до цифри 7. Для цього іноді

треба багато спроб. Але гра того варта. Учасники міцно усвідомлять, що знання правил і дотримання їх – це різні речі, і тільки дотримання правил приносить винагороду. До речі, сувенірну продукцію отримують усі учасники, тому що це була просто гра.

Вправа на дотримання правил під час спілкування у соціальних мережах та обміну миттєвими повідомленнями

1. Корова

Тренер об'єднує учасників у дві групи. Для цього можна використовувати декілька варіацій: перший – другий, два овочі або два фрукти. Учасники обирають з двох овочів чи фруктів улюблений, і тренер об'єднує учасників у дві команди. Учасники сідають на стільці по двоє спинами один до одного. Один із учасників отримує чистий аркуш паперу та олівець. Інший – заздалегідь підготовлений малюнок корови.

Учасник, який має малюнок, не повинен показувати його своєму партнерові, а виключно словами передати зміст зображеного. Учасник, який має чистий аркуш паперу та олівець, повинен якомога точніше намалювати те, що буде казати його напарник, тобто зробити свою копію малюнка.

Задля гарної мотивації тренер повідомляє, що у випадку, коли оригінал і копія малюнка будуть дуже схожі або ідентичні, обидва переможці отримають приз, наприклад, мобільний телефон. Учасникам для роботи відводиться 3 хвилини.

Звісно, всі учасники змалювали корів, але малюнки мали відмінності.

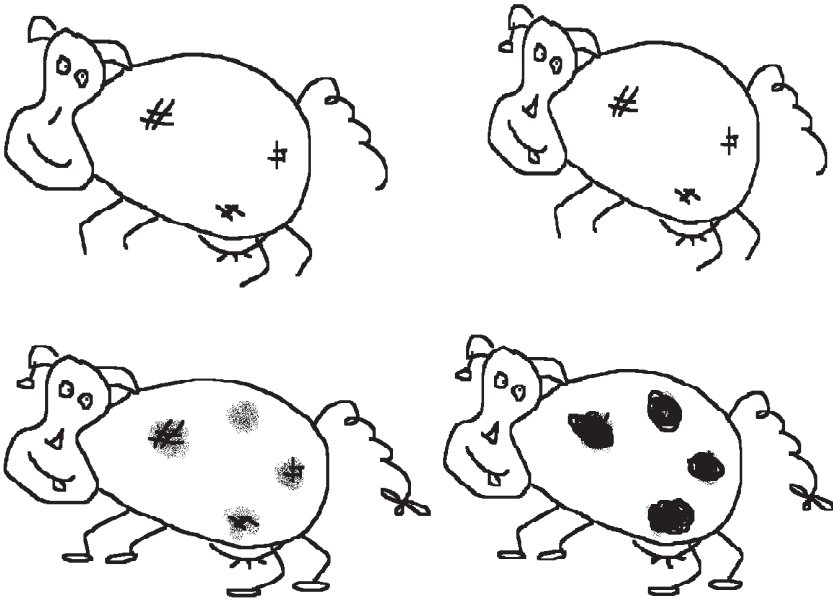
Під час аналізу гри тренер не знайде двох однакових малюнків – всі вони будуть дуже різними.

Тренер запитує в учасника, який повинен був передати словами зміст зображення: «Чи це ти так радив малювати?», «Тоді чому твій напарник намалював зовсім не те, що ти йому говорив?». Потім тренер звертається до учасника, який малював: «Чи дійсно ти малював те, що він тобі казав? Чому ж тоді у вас неоднакові малюнки?».

Учасники під час аналізу гри мають самостійно дійти висновку, що неможливо отримати однакові малюнки, бо кожен буде переказувати зміст зображеного та малювати по-своєму, адже у кожного своя уява.

Сенс гри полягає в тому, щоб усвідомити, що не можна довіряти інформації, отриманій лише завдяки одному органу чуття (в даному випадку – слуху). Тоді чому ми довіряємо інформації, яку отримуємо від співрозмовників у соціальних мережах? Ми не бачимо їх, не відчуваємо їхньої реакції, навіть не можемо бути впевненими, що фотографія та реальна людина по той бік екрана будуть схожі. Ми не знаємо, хто саме знаходиться по той бік монітора.

Головне у грі – не забути, що учасники змагаються не за кращий малюнок, а за точність передачі зображення. Тому корова повинна бути зображена просто, схематично, аби учасники, котрі не мають художнього хисту, також мали змогу її відтворити.



2. Хор тварин

Тренер заздалегідь готує 5-6 аркушів паперу форматом А-4 із зображенням тварин: корови, осла, собаки, kota, кози, свині.

Учасники об'єднуються у групи. Лідер команди витягує один аркуш із зображенням тварини.

Завдання для команд. Необхідно проспівати декілька куплетів відомої пісні мовою тварини, яку вони обрали.

Обговорення.

- Чи легко було виконати це завдання? Чому?
- Чи легко було зрозуміти іншу команду? Чому?

Аналогія з Інтернетом.

Спілкуючись у соціальних мережах або за допомогою миттєвих повідомлень у мережі Інтернет, ми зустрічаємо незнайомі нам вислови або символи. Це певний сленг, який треба знати, якщо хочеш зрозуміти співрозмовника.

3. Автобус

Учасники об'єднуються у дві команди.

Одна команда повинна розподілити ролі для імітації автобуса: водій, сидіння, кондуктор, склоочисники, фари, двигун, двері, кермо, пасажирки, аптечка, квитки тощо. Учасники цієї команди повинні рухами показати одну-єдину картину – автобус, який рухається. Завдання для іншої команди – визначити ролі кожного учасника.

Обговорення.

- Чи легко було виконати це завдання? Чому?
- Чи легко було зрозуміти іншу команду? Чому?

Аналогія з Інтернетом.

Спілкуючись у соціальних мережах або за допомогою миттєвих повідомлень у мережі Інтернет, ми зустрічаємо цікаві, а іноді й незрозумілі нам слова та форми поведінки. Треба бути дуже уважним, аби знайти в цьому сенс. Іноді це дуже важко зробити, бо ми не можемо знати думок цих людей та мотивів їхньої поведінки. Тому у більшості випадків непотрібно приєднуватися до незрозумілих угруповань.

Вправи на формування навичок безпечної поведінки у випадку потрапляння на сайти із дорослим контентом та контентом, який є небажаним для дітей.

1. Термінатор

Кількість учасників гри повинна бути кратна трьом. Тренер пояснює правила. Всі учасники беруть участь у грі. Вони отримують стікери різного кольору і наклеюють їх на свій одяг. Завдання полягає в тому, щоб не загубити і не втратити ці стікери. Тренер буде показувати

на будь-кого з учасників та давати команди: «міксер!», «пральна машинка!», «слон!», «тостер!».

На кожну команду всі учасники повинні виконати відповідні дії. Наприклад, тренер показує на одного учасника та промовляє: «Міксер!» Учасник, на якого показав тренер, піднімає руки та промовляє голосно звук «вжик», а учасники зліва та справа рухаються навколо своєї осі під його руками. Усі інші пропорційно розміщуються по троє і також виконують ці дії.

Якщо лунає команда «пральна машинка!», учасник, на якого показав тренер, починає крутити головою, а ті, що знаходяться зліва та справа, руками роблять велике коло, в якому і крутить головою їхній партнер по грі. Всі інші учасники пропорційно розміщуються по троє і також виконують ці дії.

Команда «слон!», і учасник, на якого показав тренер, витягує вперед складені руки («хобот»), а учасники зліва та справа імітують руками великі вуха слона. Решта пропорційно розміщуються по троє і також виконують ці дії.

Звучить команда «тостер!», і учасник, на якого показав тренер, починає підстрибувати на одному місці, а учасники зліва та справа складають руки та піднімають їх вгору. Між цими руками і плигає «тост». Всі інші учасники пропорційно розміщуються по троє і також виконують ці дії.

Тренер повідомляє тільки 2-3 обраним учасникам їхнє особливе завдання. Як тільки тренер скаже «термінатор!», ці учасники повинні якомога швидше забрати стікери в інших учасників.

Коли учасники добре зрозуміли правила гри і швидко орієнтуються після кожної команди, тренер несподівано для всіх дає команду «термінатор!». Звісно, більшість учасників не розуміє, яку саме дію треба виконувати. Але в цей час 2-3 учасники, які знають нюанси гри, користуючись розгубленістю решти учасників, швидко забирають стікери, які всі, згідно з правилами, повинні пильно берегти. У результаті більшість із них втратить свої стікери – їх заберуть «термінатори», яким із самого початку були відомі всі правила гри.

Обговорення.

- Чи сподобалася вам гра? Чому? (учасники не знали всіх правил).
- Чому ви не зберегли свої стікери? Що вам заважало?
- Чи незнання правил гри може виправдати той факт, що ви не зберегли стікери, адже ви чітко знали умову гри: берегти стікери?

Аналогія з мережею Інтернет.

У більшості випадків діти, відвідуючи сайти із дорослим або небажаним для них контентом, не усвідомлюють тих небезпек, на які можуть наразитися. Мета авторів цих сайтів – ввести дітей у такий психологічний стан, щоб вони втратили пильність. Оскільки діти не знають справжньої мотивації авторів цих сайтів, вони досить легко можуть потрапити у халепу.

2. Плутанина

Тренер розставляє учасників так, щоб утворилося два кола: одне коло – в середині іншого. Після цього учасники із першого кола правою рукою повинні взяти за праву руку учасника з другого кола, причому не того, який знаходиться поруч, а того, що навпроти. Таким чином утворюється плутанина.

Завдання. Не відпускаючи, рук необхідно всім розплутатися. Можна переступати один через одного, повертатися, але не відпускати рук.

Обговорення.

- Чи легко було виконати завдання? Чому?

Аналогія з мережею Інтернет.

Іноді ми можемо заплутатися у великій кількості ресурсів Інтернету або потрапити на сайти із небажаним контентом. Але виплутатися завжди можна: потрібні лише бажання та терплячість.

Вправи на формування навичок безпечної поведінки під час обміну фотографіями та особистою інформацією

1. Таємниця

Тренер просить усіх учасників сісти на стільці. Кожен отримує аркуш паперу та олівець.

Тренер нагадує про те, що кожен із учасників має певні таємниці і не хоче, щоб вони стали відомі іншим. Наприклад: ми користувалися не своїми речами, без дозволу брали чужі речі, плітували про кращого друга тощо. Це може статися з кожним: з ким - частіше, а з ким - дуже рідко, але це трапляється.

Тренер просить описати на папері одну таку подію. Після того, як учасники напишуть, тренер просить дуже щільно скласти цей папірець, перегнувши декілька разів, щоб не було видно, що саме написано, і покласти його під стілець.

Після цього всім учасникам пропонується пересісти на два стільці вправо, потім на п'ять стільців вліво та ще на три стільці вліво.

Обговорення.

- Що Ви зараз відчуваєте?

- Чи можете ви визначити, під яким стільцем знаходиться ваша таємниця? У більшості випадків учасники скажуть «так», бо будуть ретельно стежити за своїм папірцем.

Тренер просить взяти чужий папірець під стільцем, на якому він зараз опинився. Не треба його розгортати! Учасники лише беруть у руки папірці з чужими таємницями.

- Що ви відчуваєте тепер? Чи хотіли б ви, щоб зараз хтось прочитав зміст того, що написано на папері, який він тримає у руках? Звісно, ніхто цього не бажає.

Аналогія з мережею Інтернет.

Досить часто ми розміщуємо у мережі Інтернет інформацію, яка може нас компрометувати або навіть ідентифікувати: повне ім'я, домашню адресу, телефон, фінансовий статок, місце роботи батьків та інше. Цього не варто робити, інакше ми не будемо почувати себе так, як під час цієї вправи.

Увага! Ця вправа проводиться з дітьми, старшими за 12 років, або дорослими. Тренер повинен уважно слідкувати, щоб учасники навіть випадково не дізналися про зміст написаного на папірцях. Одразу після завершення вправи всі папірці збираються і на очах учасників знищуються або скидаються в кошик для сміття. Це необхідно зробити, адже вправа наочно демонструє ризик розміщення приватної інформації в мережі Інтернет, але кожен учасник повинен бути впевненим: його таємниця не стала відома іншим.

2. Гніздо

Усі учасники, крім одного, отримують по 1 газеті. Газета – це і є «гніздо». Учасники – «птахи». Завдання «птахів» – розстелити газету та сісти у своє «гніздо». Але один учасник залишився без «гнізда».

Тренер дає команду «переліт!». По цій команді учасники повинні змінити свої «гнізда». Той, хто не встиг це зробити, стає ведучим гри.

Гра розрахована на дітей віком від 12 років та дорослих. Під час гри тренер чекає моменту, коли учасники, знаходячись у своїх «гніздах», поглядом будуть шукати собі пару для швидкого обміну «гніздами». Це і є головний момент вправи: дочекатися, коли учасники почнуть поглядом визначати собі партнера для обміну.

Аналогія з мережею Інтернет.

У мережі Інтернет дуже швидко все змінюється. Лише той, хто миттєво орієнтується, буде мати «бонуси» від Інтернету: за мінімальний час отримуватиме максимум безпечної та корисної інформації. А той, хто не розуміє цих правил, буде постійно втрачати своє «гніздо».

Зоровий контакт сприяє встановленню довіри між людьми. Лише після встановлення довірливих відносин ми можемо надавати персональну інформацію про себе (як аналогія: під час вправи учасники поглядом домовляються про обмін «гніздами»).

Вправа на формування навичок безпечної поведінки при користуванні електронною поштою

Тілоохоронці

Тренер просить вийти до нього 6 учасників. Кожен з них отримує свою роль, написану на аркуші паперу форматом А-4: «Оля», «Охоронець» - 3 хлопці, «Хуліган», «Вірус» - 1 дівчина.

Тренер розповідає історію про відому VIP-персону «Олю». «Оля» знаходиться посеред приміщення. Її охороняють три «охоронці». Їхнє завдання - не підпустити «хулігана» до «Олі». Завдання «хулігана» - доторкнутися до «Олі». Тренер пропонує «Хулігану» спробувати доторкнутися до «Олі». Звісно, це неможливо, бо три хлопці-«охоронці» сумлінно виконують свої обов'язки. Але в цей час у гру вступає «вірус», який торкається до «охоронців», і вони «починають хворіти» - виходять із гри. «Оля» залишається сама. Питання до всіх учасників-глядачів: «Що тепер заважає «хулігану» доторкнутися до «Олі»? (Нічого).

Обговорення.

Запитання до «Олі»:

- Як ви себе почували в оточенні трьох «охоронців»?

Запитання до «хулігана»:

- Як ви себе почували, коли ми запропонували вам доторкнутися до «Олі», яка була оточена «охоронцями»?

Запитання до «Олі»:

- Як ви себе почували, коли ваші «охоронці» зникли?

Аналогія з мережею Інтернет.

Усі ми користуємося електронною поштою. Ми відчуваємося дуже комфортно, коли знаємо, що наші листи захищені. Якщо ж наша

охорона (брандмауер) вимкнута, ми одразу наражаємося на реальну небезпеку: в будь-який час до нас може «завітати» «хуліган» і видалити всі наші важливі листи або скористатися нашою скринькою.

ДОДАТКОВІ МАТЕРІАЛИ ДЛЯ РОБОТИ З БАТЬКАМИ

Матеріали для підготовки інформаційних повідомлень або друкованих порад

Он-лайн-хижаки: що можуть зробити батьки, щоб мінімізувати цей ризик?

Використання таких інструментів комунікації в Інтернеті, як чат-кімнати, електронна пошта та обмін миттєвими повідомленнями, може поставити дитину під потенційну загрозу зустрічі з он-лайн-хижаками. Анонімність Інтернету означає, що довіра та тісний зв'язок в он-лайні можуть виникати досить швидко. Хижаки користуються цією анонімністю, щоб будувати свої взаємовідносини з недосвідченими молодими людьми. Батьки можуть захистити своїх дітей, якщо вони будуть обізнані з ризиками он-лайн-спілкування та цікавитимуться діяльністю своїх дітей у мережі Інтернет.

Батькам потрібно бути добре поінформованими, щоб отримати відповіді на свої запитання про те, як діють он-лайн-хижаки, хто ризикує стати їхньою жертвою та як знизити для своєї дитини ризик стати мішенню інформаційних атак.

Як діють он-лайн-хижаки?

Хижаки встановлюють контакт із дітьми шляхом розмов у чат-кімнатах, обміну миттєвими повідомленнями, завдяки електронній пошті або дошкам повідомлень. Багато підлітків користуються он-лайн-форумами підтримки ровесників для розв'язання своїх проблем. Хижаки часто відвідують такі зони в он-лайні для пошуку вразливих жертв.

Он-лайн-хижаки намагаються поступово спокусити своїх жертв, виявляючи по відношенню до них увагу, доброту або навіть пропонуючи подарунки. Як правило, не шкодують ні часу, ні грошей, ні енергії. Вони в курсі найостанніших музичних новинок і все знають про хобі, які цікавлять дітей. Вони вислуховують дітей і співчують їхнім

проблемам, намагаються «послабити комплекси» молодих людей, поступово вводючи у свої розмови сексуальний контекст або показуючи їм відверто сексуальні матеріали.

Деякі он-лайн-хижакі намагаються одразу ж втягнути дітей у відверто сексуальні розмови. Цей більш прямолінійний підхід може включати і сексуальне домагання. Хижакі також можуть запрошувати дітей, з якими вони знайомляться в он-лайні, до контакту віч-на-віч.

Хто ризикує стати жертвою он-лайн-хижаків?

Юнаки та дівчата є найбільш вразливою категорією, яка знаходиться під загрозою контактів з он-лайн-хижакіми. Молодь досліджує свою сексуальність, виходить з-під батьківського контролю й шукає нових стосунків за межами сім'ї. Виходячи в Інтернет під маскою анонімності, вони, скоріш за все, ризикують стати чиймись жертвами в он-лайні, цілком не розуміючи до кінця можливих наслідків.

Молоді люди, які є найбільш вразливими для он-лайн-хижаків, мають наступні риси:

- Вони новачки в он-лайні й незнайомі з «мережесим'ю».
- Завзяті користувачі комп'ютера.
- Хочуть спробувати щось нове, авантюрно у житті.
- Активно шукають уваги та теплих стосунків.
- Бунтівні.
- Ізольовані або самотні.
- Допитливі.
- Збентежені в плані статевої приналежності.
- Занадто довірливі, яких можна легко ошукати.
- Їх приваблюють субкультури, що існують за межами їхнього контрольованого батьками світу.

Діти вважають, що вони знають про всю небезпеку хижаків, але насправді вони наївні, коли мова йде про он-лайн-стосунки.



Як батьки можуть мінімізувати ризик для своїх дітей?

- *Поговоріть зі своїми дітьми про он-лайн-хижаків і потенційну небезпеку від них.*
- *Малі діти не повинні використовувати чат-кімнати — небезпека там є надто великою. У міру того, як діти*

дорослішають, направляйте їх на добре контрольовані дитячі чат-кімнати. Заохочуйте навіть підлітків до використання контрольованих чат-кімнат.

- Якщо ваша дитина використовує чат-кімнати, переконайтеся, що ви знаєте, які з них вона відвідує і з ким вона розмовляє. Слідкуйте й самі за зонами розмов, щоб розуміти, на які теми там спілкуються.
- Порадьте своїм дітям ніколи не залишати публічної зони чат-кімнати. Багато чат-кімнат пропонують приватні зони, де користувачі можуть спілкуватися з іншими віч-на-віч, і монітори чату не можуть читати ці повідомлення. Ці зони ще часто називаються «зонами шепотіння».
- Тримайте комп'ютер, підключений до Інтернету, у загальній зоні своєї оселі, і ніколи — у кімнаті дитини. Он-лайн-хижакам набагато важче встановити зв'язок із дитиною, якщо екран комп'ютера знаходиться на видному місці. Але навіть якщо екран комп'ютера встановлений у загальній зоні вашої оселі, знаходьтеся поряд з вашою дитиною, коли вона виходить в он-лайн.
- Якщо ваші діти ще малі, вони повинні користуватися сімейною адресою електронної пошти і не мати власних облікових записів. Коли вони підростуть, ви можете попросити провайдера послуг Інтернету (ISP) встановити для них окрему адресу електронної пошти, але пошта ваших дітей повнна залишатися у вашій скриньці.
- Накажіть вашим дітям ніколи не відповідати на миттєві повідомлення або електронну пошту, що надійшли від незнайомих. Якщо ваші діти використовують комп'ютери у місцях, які знаходяться за межами вашого контролю: у публічній бібліотеці, у школі, у будинку друзів, — з'ясуйте, які там встановлені засоби комп'ютерного захисту.
- Якщо всі запобіжні заходи виявилися марними, і ваші діти зустрілися з он-лайн-хижаком, не звинувачуйте їх. Вдайтеся до рішучих дій, щоб зашкодити подальшим зустрічам вашої дитини з цією особою.

Що порадити дітям, щоб вони не стали жертвою он-лайн-хижаків?

Існує багато запобіжних заходів, якими можуть скористатися ваші діти. Дайте їм такі настанови.

- Ніколи не завантажуйте картинки з незнайомих джерел - вони можуть мати відверто сексуальний зміст.
- Використовуйте фільтри електронної пошти
<http://www.microsoft.com/athome/security/email/fightspam.msp>.
- Завжди і негайно повідомляйте дорослих, якщо в он-лайні щось примушує вас почуватися некомфортно або лякає.
- Вибирайте статево нейтральне екранне ім'я, яке не містить сексуального підтексту і не відображає ніякої персональної інформації.
- Ніколи і нікому в он-лайні не повідомляйте свою персональну інформацію (включаючи вік та стать) або інформацію про свою родину та не заповнюйте персональні профілі.
- Припиняйте будь-яке спілкування через електронну пошту та обмін миттєвими повідомленнями або розмови в чатах, якщо хтось починає ставити вам запитання, які є занадто особистими або мають сексуальний підтекст.
- Розмістіть поряд з комп'ютером сімейну угоду про роботу в он-лайні, яка буде нагадувати вам про захист від небезпеки в Інтернеті.

Як батьки можуть визначити, що на дитину "полюють" он-лайн-хижаки?

Можливо, дитина стала мішенню он-лайн-хижака, якщо в її поведінці спостерігається наступне.

- Вона проводить занадто багато часу в он-лайні. Більшість дітей, які стали жертвами он-лайн-хижаків, проводять багато часу в чат-кімнатах і можуть зачиняти двері до своєї кімнати та робити секрет з того, чим вони займаються, коли сидять за своїм комп'ютером.
- Батьки знаходять порнографію в сімейному комп'ютері. Хижаки часто використовують її для того, щоб відкрити шлях до сексуальних розмов, зробити дітей своїми сексуальними

жертвами, постачаючи їм Web-сайти, фотографії та повідомлення електронної пошти сексуального змісту. Хижаки можуть використовувати фотографії з дитячою порнографією, щоб переконати дітей, що секс дорослих людей з дітьми - це нормально. Батьки повинні знати, що діти можуть ховати порнографічні файли на дисках, особливо якщо інші члени сім'ї користуються комп'ютером.

- Дитина отримує телефонні дзвінки від людей, яких батьки не знають (іноді з віддаленого місця) або з невідомих номерів. Після встановлення контакту з дитиною в он-лайн деякі он-лайн-хижаки можуть спробувати зв'язатися з дітьми для того, щоб залучити їх до телефонного сексу або навіть запропонувати зустрітися віч-на-віч. Якщо діти сумніваються, давати чи не давати свої домашні телефонні номери, то он-лайн-хижаки запропонують свої. Деякі з них навіть мають безкоштовні номери для тих, хто телефонує. Таким чином, потенційні жертви можуть телефонувати їм, але батьки про це можуть не знати. Інші можуть запропонувати дітям номер, дзвінок на який оплачується абонентом, і де висвічується телефонний номер того, хто телефонує. У такий спосіб хижаки отримують телефонні номери дітей. Батьки не повинні дозволяти своїй дитині без їхнього нагляду особисто зустрічатися з людьми, з якими вона познайомилася в он-лайні.

- Дитина отримує пошту, подарунки або пакунки від людини, яку ви не знаєте. Хижаки часто надсилають листи, фотографії та подарунки потенційним жертвам. Он-лайн-хижаки навіть відправляють квитки на літак, щоб заохотити дитину зустрітися з ними особисто.

- Дитина уникає сім'ї та друзів або швидко вимикає монітор чи змінює вміст екрана, якщо хтось із дорослих входить до кімнати. Он-лайн-хижаки активно працюють над тим, щоб вклинитися між дітьми та їхніми сім'ями, часто навмисне перебільшуючи їхні незначні домашні проблеми. Діти, які стали сексуальними жертвами, уникають інших та перебувають у депресії.

- Дитина використовує чийсь обліковий запис в он-лайні. Навіть ті діти, які не мають доступу до Інтернету вдома,

можуть зустрітися з негідником в он-лайні, перебуваючи у друзів або в громадському місці, навіть у бібліотеці. Хижаки інколи надають дітям облікові записи, щоб з ними можна було зв'язатися.



Як батьки можуть допомогти дитині, якщо вона стала жертвою он-лайн-хижаків?

- Якщо дитина отримує відверто сексуальні фотографії від он-лайн-співрозмовника або сексуальні пропозиції через електронну пошту, миттєві повідомлення або в інший спосіб, зверніться до міліції. Збережіть будь-які документальні свідчення, включаючи адреси електронної пошти, адреси Web-сайтів та імена в чаті, щоб передати їх правоохоронцям.
- Перевірте, чи немає на вашому комп'ютері порнографічних файлів або сексуального спілкування будь-якого типу. Це може бути попереджувальною ознакою того, що на дитину «полюють» он-лайн-хижаки.
- Слідкуйте за доступом вашої дитини до всіх видів живого он-лайн-спілкування, таких, як чат-кімнати, обмін миттєвими повідомленнями або електронна пошта. Он-лайн-хижаки зазвичай знайомляться з потенційними жертвами спочатку у чат-кімнатах, а потім продовжують спілкуватися з ними через електронну пошту або за допомогою миттєвих повідомлень.



Як убезпечити дитину від Інтернет-залежності?

Не можна дозволяти дитині проводити занадто багато часу в он-лайні.

Кількість часу, яку діти проводять в он-лайні, є причиною хвилювання багатьох батьків. Спочатку батьки з радістю прийняли Інтернет у свої оселі, сподіваючись, що він відкриє нові навчальні можливості для їхніх дітей. Однак дуже швидко батьки збагнули: замість того, щоб використовувати Інтернет для виконання домашніх завдань і досліджень, діти проводять там години, обмінюючись миттєвими повідомленнями зі своїми друзями, граючись в он-лайн-ігри або розмовляючи з незнайомими людьми у чат-кімнатах.

Підтримання здорового балансу між розвагами та іншими видами діяльності в житті дітей було завжди проблемою для батьків. Інтернет

зробив це завдання ще більш складним. Можливості, які надає Інтернет для спілкування та он-лайн-ігор, іноді призводять до того, що багато дітей і підлітків втрачають відчуття часу, знаходячись в он-лайні. Ось кілька порад для батьків, як допомогти дітям позбутися Інтернет-залежності.

- *Придивіться, чи є у вашої дитини симптоми Інтернет-залежності. Запитайте себе, чи позначається використання Інтернету вашою дитиною на її шкільній успішності, здоров'ї, стосунках із членами родини та друзями. Визначте, скільки часу ваші діти проводять в он-лайні.*
- *Якщо ваша дитина демонструє серйозні ознаки Інтернет-залежності, зверніться за професійною допомогою та отримайте консультацію спеціаліста. Маніакальне використання Інтернету може бути симптомом інших проблем вашої дитини, зокрема депресії, агресивності або низької самооцінки.*
- *Перевірте свої власні он-лайн-звички. Чи є у вас проблеми з контролем за власним використанням Інтернету? Пам'ятайте, що для вашої дитини ви є головним прикладом для наслідування.*
- *Не забороняйте Інтернет. Він є важливою частиною соціального життя більшості дітей. Натомість встановіть сімейні правила використання Інтернету та визначте, які сайти може та які не може відвідувати ваша дитина. Слідкуйте, щоб вона дотримувалася цих правил. Вони можуть обмежувати час, протягом якого дитина перебуває в он-лайні кожного дня, забороняти використання Інтернету або обмін миттєвими повідомленнями, доки вона не зробила домашні завдання, не дозволяти спілкуватися в чат-кімнатах або заходити на сайти, призначені для дорослих.*
- *Тримайте комп'ютер у відкритій зоні помешкання, а не в дитячій кімнаті.*
- *Заохочуйте та підтримуйте участь вашої дитини в інших видах діяльності, особливо фізичних заняттях та іграх з іншими дітьми.*
- *Допомагайте вашим дітям налагодити спілкування з іншими людьми в реальному житті. Якщо ваша дитина сором'язлива або ніяковіє, спілкуючись із ровесниками, віддайте її на*

заняття, які допоможуть набути навичок спілкування. Заохочуйте ті види діяльності, які можуть сприяти спілкуванню вашої дитини з іншими дітьми, котрі мають схожі інтереси та хобі.

- *Контролюйте своїх дітей. Вивчіть програми, які проводять моніторинг та обмежують використання Інтернету, такі, як батьківські контролю, включені до сервісу MSN Premium (EN) <http://join.msn.com/>.*

- *Пропонуйте альтернативи. Якщо вам здається, що вашу дитину цікавлять лише он-лайн-відеоігри, спробуйте призвичаїти її до оф-лайнових «замінників» улюблених ігор. Наприклад, якщо вашій дитині подобаються рольові ігри у стилі фентезі, заохочуйте її читати книжки з фентезі.*



10 правил, яким потрібно навчити дітей, щоб підвищити їхню безпеку у Web

Інтернет може бути прекрасним місцем для навчання дітей, їхнього дозвілля та розваг, спілкування зі шкільними друзями або просто місцем, де вони можуть відпочивати чи щось досліджувати. Але, як було сказано вище, всесвітня павутина може бути небезпечною для дітей. Перш ніж ви дозволите дитині виходити в он-лайн без вашого нагляду, встановіть правила користування Інтернетом і домовтеся з дитиною, що вона буде їх дотримуватися.

Якщо ви не знаєте, з чого почати, ось кілька порад, які допоможуть навчити дітей безпечно користуватися Інтернетом.

1. *Заохочуйте свою дитину ділитися з вами своїм досвідом роботи в Інтернеті. Насолоджуйтеся Інтернетом разом зі своїми дітьми.*

2. *Привчайте своїх дітей довіряти інтуїції. Якщо щось в он-лайні примушує їх нервувати, вони повинні вам про це повідомити.*

3. *Якщо ваші діти відвідують чат-кімнати, використовують програми обміну миттєвими повідомленнями (EN) <http://www.microsoft.com/athome/security/online/imsafety.mspx>, грають в он-лайні у відеоігри або роблять щось інше в Інтернеті, для цього вимагається ім'я користувача, за яким його можна було б ідентифікувати. Допоможіть дітям правильно вибрати ім'я*

й перевірте, щоб воно не відображало ніякої особистої інформації про них.

4. Наполягайте на тому, щоб ваші діти ніколи не давали своєї адреси, номера телефону або іншої персональної інформації, включаючи інформацію про те, в яку школу вони ходять або де їм подобається гратися чи відпочивати.

5. Поясніть своїм дітям, що різниця між правильним і неправильним в Інтернеті така ж, як і в реальному житті.

6. Розкажіть своїм дітям, як виявляти повагу до інших в он-лайні. Переконайте їх, що правил культурної поведінки треба дотримуватися не тільки в реальному житті, але й тоді, коли знаходишся за комп'ютером.

7. Виховуйте у ваших дітей повагу до чужої власності в он-лайні. Поясніть їм, що створення незаконних копій творів інших людей: музики, відеоігор, програм - це все одно, що крадіжка товару в магазині.

8. Накажіть своїм дітям ніколи не зустрічатися зі своїми он-лайн-друзями особисто. Поясніть їм, що вони можуть бути не тими, за кого себе видають.

9. Попередьте своїх дітей, що не все, що вони читають або бачать в он-лайні, є правдивим. Заохочуйте їх запитувати про це, якщо вони в чомусь невпевнені.

10. Контролюйте, що роблять ваші діти в он-лайні, за допомогою найсучасніших програм Інтернету. Батьківський контроль може допомогти фільтрувати шкідливий вміст, здійснювати моніторинг сайтів, які відвідують ваші діти, та з'ясовувати, що вони там роблять.



Як навчити дітей уникати в он-лайні неправдивої інформації?

Інтернет пропонує незліченні ресурси та фантастичні можливості для навчання, але він також містить велику кількість інформації, яка не може бути ані корисною, ані надійною. Оскільки будь-хто може розміщувати коментарі або інформацію в Інтернеті, користувачам необхідно розвивати навички критичного мислення, щоб оцінювати правильність он-лайн-інформації.

Поясніть своїм дітям, як працює Інтернет, і розкажіть, що Web-сайти може створювати будь-хто. Навчіть їх користуватися широким колом інформаційних ресурсів, щоб вони могли перевіряти правильність та достовірність того, що бачать в он-лайні.



Як навчити дітей перевіряти достовірність та правдивість інформації?

- *Починайте їх навчати цьому ще в ранньому віці. Навіть дошкільнята зараз використовують Інтернет для того, щоб шукати інформацію, тому важливо якомога раніше навчити їх відрізняти факти від чийхось припущень чи пропаганди, розпізнавати упередженість або стереотипи.*
- *Навчайте ваших дітей аналізувати інформацію, яку вони знаходять в он-лайні. Наприклад: яке призначення цього сайту? чи містить сайт контактну інформацію та відомості про автора? чи спонсорується сайт якоюсь компанією або людиною? чи це публічне спілкування? чи є Інтернет найкращим місцем для пошуку тієї інформації, яка тобі потрібна?*
- *Переконайтеся, що ваші діти звіряють інформацію, яку вони знайшли в он-лайні, з іншими джерелами з метою перевірки її достовірності. Пошліться на інші Web-сайти або засоби масової інформації (газети, журнали та книги) з метою перевірки інформації. Перевіряйте її разом з дітьми.*
- *Заохочуйте дітей використовувати різноманітні інформаційні джерела, а не тільки Інтернет. Відведіть їх до бібліотеки. Також розгляньте варіант покупки хорошої енциклопедії на CD-ROM, наприклад, Microsoft Encarta (EN) <http://www.microsoft.com/products/encarta/default.msp>. Це відкриє дітям доступ до альтернативних джерел інформації.*
- *Навчіть своїх дітей технікам ефективного пошуку інформації в он-лайні. Це значно розширить їхні можливості в отриманні якісної інформації. Запропонуйте дітям використовувати різноманітні пошукові сервери, замість того, щоб користуватися одним-єдиним сайтом.*
- *Виховуйте у дітей негативне ставлення до матеріалів, що містять елементи жорстокості чи насилля. Програмні фільтри можуть допомогти заблокувати деякі з них. Однак*

ваші діти мають знати про події, що відбуваються у світі, щоб відрізнити шкідливу та неправдиву інформацію від позитивної та корисної.



Як захистити дітей від матеріалів Інтернету, що пропагують насилля, жорстокість та непримириме ставлення до інших людей?

В Інтернеті існує багато форм прояву агресії та ненависті, починаючи від терористичних сайтів і закінчуючи сайтами, що містять жорстку сатиру. Неважко зрозуміти, як деякі діти переходять від сайтів, де глузують з інших людей через їхню зовнішність, до сайтів, де об'єктом нападів стають національні та сексуальні меншини.

Приблизники різних угруповань, які пропагують непримириме ставлення до інших людей або груп людей, все більше проникають в Інтернет, щоб залучити до своїх лав молодь. Роздмухувачі національної ненависті та негативного ставлення до інших спільнот шукають вразливих юнаків, яких можна залучити до свого угруповання через приватні чат-кімнати та електронну пошту. Щоб заманити до себе молодих людей, вони використовують навіть музичні твори з негативним ідейним змістом. Коли діти шукають музику в мережі, вони можуть легко натрапити на сайти, які продають такі пісні або пропонують їх безкоштовно.

Як допомогти дітям уникнути шкідливої та небезпечної інформації, яка негативно впливає на їхнє фізичне і психічне здоров'я та морально-психологічний стан?

Батьки повинні захистити своїх молодших дітей від такої інформації в Інтернеті. Вони також повинні навчити більш дорослих дітей критично ставитися до он-лайн-матеріалів. Ось декілька підказок, якими ви можете скористатися, щоб допомогти своїм дітям уникнути небезпечних Інтернет-ресурсів. Для отримання більш конкретної інформації про те, як можна захистити своїх дітей, прочитайте "Посібник з безпечної роботи в он-лайні для батьків" <http://www.microsoft.com/ukraine/athome/security/children/parentsguide.mspx>.

- *Дізнайтеся все, що можна, про Інтернет і про те, що ваші діти роблять в он-лайні. Попросіть своїх дітей показати вам, які місця вони там відвідують і що їм подобається. Ваше спілкування повинне бути відвертим, щоб ваші діти могли без вагань прийти до вас за допомогою, якщо їх щось стурбує.*

- Укладіть з вашими дітьми угоду про роботу в он-лайн. Угода має містити чіткі інструкції щодо того, які сайти діти можуть відвідувати в Інтернеті і що вони там можуть робити.
- Стежте з використанням Інтернету вашими дітьми. В основному, діти, молодші 10 років, не володіють навичками критичного мислення, і тому для них небезпечно перебувати у мережі самим. Крім того, потрібно тримати комп'ютери, приєднані до Інтернету, у відкритій зоні вашої оселі, а не в дитячій кімнаті.
- Розкажіть своїм дітям про можливі прояви ненависті, агресії та ворожого ставлення до інших людей в он-лайн. Молоді люди краще зможуть уникнути такої інформації, якщо ви розкажете про стратегію людей, які пропагують насилля, розпусту, жорстокість, расизм, націоналізм тощо та поясните, що означають ці поняття. Навчіть дітей розпізнати інформацію з негативним контекстом на Web-сайтах та символи різних етнічних та расистських угруповань.
- Дізнайтеся про програми фільтрації. Фільтри можуть допомогти заблокувати певні небезпечні матеріали, але, на жаль, не вирішують проблему остаточно. Іноді негативні матеріали просочуються в Інтернет у таких формах, що їх важко розрізнити і заблокувати за допомогою фільтрів.
- Прищеплюйте своїм дітям норми гарної поведінки в Інтернеті. Заохочуйте їх бути добрими та ввічливими, коли вони спілкуються в он-лайн, і поясніть, що неприпустимо висловлювати у своїх повідомленнях, які вони відправляють іншим людям, негативні почуття: злість, образу тощо. Нагадайте їм, що ніяка інформація в Інтернеті не може бути цілком приватною.

Діти та Інтернет: найбільш розповсюджені запитання, які ми чуємо від батьків

В якому віці можна дозволити дитині виходити в Інтернет?

Діти виходять в он-лайн з кожним роком все раніше. Найбільш швидко зростаючим сегментом користувачів Інтернету сьогодні є дошкільнята. Багато дітей використовує Інтернет у школі до досягнення

6-річного віку, і вони, напевно, захочуть виходити в он-лайн і вдома. Водночас діти, молодші 10 років, ще не мають навичок критичного мислення, тому для них небезпечно знаходитися в он-лайні самим. Ви повинні завжди бути поруч із вашими дітьми, коли вони виходять в Інтернет. Перевіряйте, щоб вони відвідували лише ті сайти, які ви вибрали. Забороніть їм ділитися персональною інформацією через Інтернет.

Чи можна дітям мати власні облікові записи електронної пошти?

Діти молодшого шкільного віку мають користуватися спільною сімейною адресою електронної пошти, а не власною. Коли вони стануть дорослішими і захочуть мати більше незалежності, ви зможете дати їм власну адресу. Пошта все одно залишатиметься в сімейній папці вхідних повідомлень, таким чином ви зможете побачити підозрілі на вигляд повідомлення, які можуть отримати ваші діти. Запитайте у свого провайдера Інтернет-послуг, які варіанти він пропонує для сімейних облікових записів електронної пошти, та розгляньте можливість використання фільтрів, щоб запобігти надходженню спаму, повідомлень, які не запитувалися, та шахрайської пошти, створеної для викрадення вашої персональної інформації.

Якими повинні бути домашні правила використання Інтернету?

Укладіть та обговоріть із дітьми угоду про використання комп'ютера вдома. Вона повинна включати в себе права дітей та їхні обов'язки під час роботи в Інтернеті. В угоді повинно бути чітко прописано :

- на які сайти ваші діти можуть заходити в он-лайні і що вони там можуть робити;
- скільки часу вони можуть проводити в Інтернеті;

- що робити, якщо їх насторожують окремі повідомлення;
- як захистити свою персональну інформацію;
- як поводити себе безпечно в інтерактивному середовищі;
- яких правил етики потрібно дотримуватися в он-лайні;
- як користуватися чат-кімнатами, групами новин та послугами миттєвого обміну повідомленнями.

Роздрукуйте угоду і тримайте біля сімейного комп'ютера. Регулярно переглядайте її та оновлюйте, враховуючи те, що ваші діти дорослішають.

В якому віці діти можуть використовувати програми обміну миттєвими повідомленнями, такі, як MSN Messenger?

Зазначені програми діти можуть використовувати у будь-якому віці. Завдання батьків полягає в тому, щоб допомогти їм працювати безпечно та захистити свою конфіденційність, а також заохочувати відповідальне ставлення до використання технологій.

Ось деякі правила, що стосуються використання MSN Messenger.

- Не заповнюйте персональний профіль у профілі каталогу членів (бо їх може побачити будь-яка людина, яка користується цим сервісом).
- Ніколи не розмовляйте в он-лайні з тим, хто має незнайому вам адресу електронної пошти або ім'я в програмі обміну миттєвими повідомленнями. Батьки повинні регулярно перевіряти списки контактів своїх дітей, щоб переконатися, що вони знайомі з тими, з ким спілкуються їхні діти.
- Ретельно переглядайте нові запити на включення до списку друзів, перш ніж дозволити цій людині приєднатися до

списку друзів у зазначеній програмі. Якщо ви цього не хочете – клацніть, щоб заблокувати таке включення. Ніколи не використовуйте обмін миттєвими повідомленнями для того, щоб розповсюджувати чутки, плітки, або повідомленнями, що містять негативні висловлювання про інших людей.

Чи мають право батьки читати миттєві повідомлення, якими обмінюються діти в MSN Messenger?

Так, MSN Messenger налаштований таким чином, щоб автоматично зберігати розмови за допомогою миттєвих повідомлень у папці на вашому комп'ютері. За замовчуванням ця папка знаходиться зазвичай у: C:\My Documents\ (Для того, щоб подивитися, де конкретно знаходиться ця папка, відкрийте MSN Messenger, клацніть на меню «Інструменти», потім «Опції», а потім переходьте до ярличка «Повідомлення»).

Пам'ятайте, що діти легко можуть відключити функцію, яка зберігає розмови у програмі обміну миттєвими повідомленнями. У такому випадку відверта розмова з вашими дітьми є набагато конструктивнішою, ніж шпигування за ними. Пам'ятайте, що вони завжди будуть на крок попереду нас, коли йдеться про комп'ютерні технології. Довіряйте дітям, але слідкуйте, щоб вони дотримувалися установлених вами правил під час роботи з комп'ютером. Переглядайте час від часу ці правила та обговорюйте їх із дітьми.

Чи можна уникнути саморозкривних вікон на домашньому комп'ютері?

Найпростіший шлях уникнення саморозкривних вікон — це використання блокуючих програм. Якщо у вас найостанніша версія Windows 7 (EN), то Internet Explorer (ваш Web-браузер) вже обладнаний блокувальником саморозкривних вікон.

Як убезпечити дітей від Інтернет-залежності?

Інтернет є прекрасним інструментом для розвитку та спілкування молодих людей, особливо для тих, хто відчуває труднощі у спілкуванні зі своїми ровесниками. Діти, які добре володіють комп'ютером, можуть користуватися популярністю в Інтернеті, підвищити свою самооцінку. Однак надмірне використання комп'ютера може ще більше ізолювати дітей, відволікати їх від інших видів діяльності, таких, як виконання домашньої роботи, заняття спортом, сон або спілкування з іншими дітьми. Батьки та вчителі зазвичай не знають, що існує така проблема, доки вона не стане серйозною. Щоб не допустити Інтернет-залежності у вашої дитини, встановіть правила використання комп'ютера вдома та збалансуйте види діяльності дитини, поєднавши роботу з комп'ютером і фізичні вправи, ігри, спілкування з однолітками тощо. Також прослідкуйте, щоб комп'ютер знаходився у відкритій зоні вашого помешкання, а не в кімнаті дитини.

Нарешті, прослідкуйте, як ви самі використовуєте Інтернет. Чи не проводите ви в он-лайні цілі години? Якщо це так, то діти, швидше за все, будуть наслідувати ваш приклад.

Що діти повинні знати про комп'ютерні віруси?

Вірус — це зловмисна комп'ютерна програма, яка вражає комп'ютерні файли або жорсткі диски комп'ютерів, а потім самокопіюється. Багато з того, чим займаються діти в он-лайні, робить комп'ютер вразливим до вірусів. Вкладення електронної пошти є найбільш розповсюдженим способом поширення вірусів, але віруси також можуть завантажуватися при спільному користуванні файлами або програмами обміну миттєвими повідомленнями. Щоб запобігти цьому, порадьте вашим дітям:

- ніколи не відкривати вкладення електронної пошти, які ви не запитували;
- сконфігурувати програму обміну миттєвими повідомленнями таким чином, щоб не можна було отримувати файли від інших користувачів;
- користуючись програмами спільного доступу до файлів, ніколи не завантажувати файли з розширенням «.exe»;
- ніколи не завантажувати ніякі програми з Інтернету без попередньої консультації з вами;
- завжди використовувати брандмауери та антивірусні програми.

Чи можна відслідковувати, які сайти відвідують діти в онлайні?

Так, існують способи відстеження сайтів, на яких перебувають ваші діти в онлайні. Але батькам треба мати на увазі, що діти, які добре розбираються в комп'ютерах, знають, як приховати свої Інтернет-стежки. Набагато ефективніше установити з дітьми довірливі стосунки та чіткі правила використання Інтернету.

Коли ви знаходитесь в Інтернеті, ваш Web-браузер (такий, як Microsoft Internet Explorer) збирає інформацію про місця, які ви відвідуєте, та зберігає її на вашому комп'ютері.

Браузери зазвичай зберігають історію нещодавно відвіданих сайтів. Більшість версій Internet Explorer мають кнопку «Історія» на верхній панелі інструментів. Якщо ви не бачите цієї кнопки, просто натисніть одночасно клавіші Ctrl (контроль) та H (P на українській розкладці), і це також видасть список сайтів, які відвідувала ваша дитина.

Браузери також роблять тимчасові копії Web-сторінок, які відомі під назвою кеш-файлів, та зберігають їх на вашому комп'ютері.

Для того, щоб переглянути тимчасові файли, виконайте наступні операції:

- В Internet Explorer натисніть «Інструменти» та виберіть «Опції Internet».
- На ярличку «Загальне», під зоною «Тимчасові файли Internet», натисніть кнопку «Налаштування».
- Під зоною «Папки тимчасових файлів Internet» натисніть кнопку «Подивитися файли».

Ви маєте побачити на своєму комп'ютері список Web-сторінок, які ви або ваші діти нещодавно відвідували, а також переглянуті картини та cookies.

Існує багато видів програм, які дозволяють вам здійснювати моніторинг різних видів он-лайн-діяльності, наприклад, MSN Premium пропонує набір батьківських контролів, які дозволяють вам фільтрувати Інтернет та посилають вам щотижневі звіти, де вказується, які сайти відвідували ваші діти в Інтернеті, з ким вони розмовляли та багато іншого.

Ви також можете навідатися до комп'ютерного магазину та скористатися тим, що вам порекомендують.

Що робити, якщо дитина стала об'єктом образ в он-лайні?

Це називається кібер-хуліганством. Таке явище дуже розповсюджене серед підлітків. Діти також можуть стати об'єктом образ, або кібер-хуліганства, коли вони грають в он-лайн-відеоігри. Якщо це трап-

ляється, ви можете заблокувати особу, котра надсилає повідомлення, які непокоять дитину. Функція блокування є в багатьох програмах обміну електронною поштою та миттєвими повідомленнями. Збережіть повідомлення образливого змісту та направте їх своєму провайдеру послуг електронної пошти. Більшість провайдерів мають відповідні політики користування, які можуть обмежити користувачів і не дозволяти їм турбувати та ображати інших по Інтернету.

Чи забезпечать дітей від негативної інформації програми фільтрації?

Інструменти фільтрації можуть бути корисними для малих дітей в якості додаткового способу батьківського контролю. Однак фільтри та блокувальники не рятують від усіх небезпек. Крім того, вони можуть блокувати багато корисних матеріалів, які потрібні вашим дітям для навчання.

Якщо дитина-підліток хоче робити покупки в он-лайн, як можна батькам переконатися, що цей сайт безпечний?

Перш ніж дозволити своїм дітям-підліткам користуватися в он-лайнні вашою кредитною карткою, ви маєте дати їм чітку інструкцію про покупки в он-лайнні та розказати, на що вони повинні звернути увагу, щоб зробити операції з грошми безпечними. Навчіть їх знаходити підказки на Web-сайті, які можуть підтвердити, що на цьому сайті можна безпечно давати інформацію про кредитну картку. Перш, ніж робити покупки на Web-сайті, знайдіть там:

- незламану іконку замка в нижньому куті сторінки, яка вказує на те, що тільки ви та Web-сайт можуть бачити цю фінансову операцію.

- «https» («s» означає «захищена»), включений до адреси Web-сайту, відображається в адресному вікні вашого браузера.

Список пунктів вгорі може бути фальшивим, і тому важливо нагадати вашим дітям, щоб вони радилися з вами, перш ніж зробити які-небудь покупки в он-лайн, тоді ви особисто зможете переконатися у безпечності сайту. Перевірте, щоб ваш браузер підтримував 128-бітне шифрування, таким чином інформація з вашої кредитної картки шифруватиметься або перемішуватиметься перед відправкою.

На що батьки повинні звертати увагу в політиці конфіденційності дитячого сайту?

Політики конфіденційності Web-сайту визначають, яким чином персональна інформація, зібрана на сайті, використовується, передається або зберігається. Для батьків важливо прочитати політику конфіденційності Web-сайту і показати своїм дітям, на що вони мають звернути увагу в цій політиці, перш ніж давати свою персональну інформацію. Іноді ці політики можуть бути занадто довгими, складними і незрозумілими.

Якщо Web-сайт не має політики або заяви про конфіденційність, будьте обережні, здійснюючи покупки або даючи персональну інформацію на цьому Web-сайті.

Коли ви читаєте політику конфіденційності, звертайте увагу на наступне:

- яка інформація про вас та ваш комп'ютер збирається та відслідковується;
- як ця інформація буде використовуватися (зокрема, чи буде вона продаватися третій стороні);
- які способи передбачено, щоб убезпечити ваших дітей у чат-кімнатах, дошках повідомлень, електронній пошті на сайті;
- чи намагається сайт отримати перевірену батьківську згоду, перш ніж дитина надасть персональну інформацію в он-лайні.

ЛІТЕРАТУРА

1. Вукіна Н.В., Дементієвська Н.П., Сукенко І.М. Критичне мислення: як цьому навчати. Науково-методичний посібник/За наук. ред. О.І.Пометун – Харків, 2007

2. Возможности и пути включения Интернет в школьное образовательное пространство / А.Л. Цветкова // Библиотеки и ассоциации в меняющемся мире: новые технологии и новые формы сотрудничества: 8-я Междунар. конф. "Крым 2001": Материалы конф. — М., 2001. — Т. 2

3. Дискурс-анализ поведения мужчин и женщин в сети / Л.Ф. Компанцева // Культура народов Причерноморья. — 2003. — N37.

4. Интерактивные технологии как средство формирования информационно-коммуникативной культуры студента-журналиста / В.В. Дмитриева // Культура народов Причерноморья.— 2004. — N49, Т.2.

5. Использование Интернет-ресурсов в образовательных целях (на основе анализа зарубежного опыта) / Е.В. Иванова // Библиотеки и ассоциации в меняющемся мире: новые технологии и новые формы сотрудничества: 8-я Междунар. конф. «Крым 2001»: Материалы конф. — М., 2001. — Т. 2.

6. Інтернет-середовище як фактор психологічного розвитку комунікативного потенціалу особистості: Автореф. дис... канд. психол. наук: 19.00.07 / В.М. Фатунова; Ін-т психології ім. Г.С.Костюка АПН України. — К., 2004.

7. Конвенція про кіберзлочинність [Електронний ресурс] / Верховна Рада України. – Електрон. текст. дані. – Режим доступу : http://zakon1.rada.gov.ua/cgi-bin/laws/main.cgi?nreg=994_575&chk=4/UMfPEGznhhqJg.ZilsJKtLHdlOUFsFgkRbI1c. – Загол. з титулу екрана.

8. Леванова, Е.А., Волошина А.Г., Плешаков В.А., Соболева А.Н., Телегина И.О. Игра в тренинге. 2-е издание. – СПб.: Питер, 2011.

9. Педагогічні засади професійного консультування молоді засобами Інтернет: Автореф. дис... канд. пед. наук: 13.00.04 / В.В. Осадчий; Вінниц. держ. пед. ун-т ім. М.Коцюбинського. — Вінниця, 2005.

10. Пилипчук А. Електронні знайомства : записки пострадавшего / А. Пилипчук // Internetua : журн. для всего офиса. – [Украина], 2007. – № 7.

11. Провинциальный студент как пользователь сети Интернет: на примере исследования студенчества Тамбовской области / Н.А. Мордасова — (Библиотеки и информационные ресурсы в современном мире науки, культуры, образования и бизнеса: 11-я Междунар. конф. «Крым 2004»: Тр. конф). — М., 2004.

12. Соціальні аспекти комунікації в мережі Інтернет: феноменологічний аналіз: автореф. дис... канд. соціол. наук: 22.00.01 / Сергій Михайлович Коноплицький; НАН України; Інститут соціології. — К., 2007.

13. Соціально-психологічні особливості формування життєвих планів Інтернет-залежної молоді: Автореф. дис... канд. психол. наук: 19.00.05 / В.В. Посохова; Ін-т соц. та політ. психології АПН України. — К., 2006.

14. Фишман С. Пойманные в сети / С. Фишман // Internetua : е-война. — [Украина], 2008. — № 1.

15. Формування культури Інтернет-комунікації майбутніх учителів засобами інформаційно-комунікаційних технологій: автореф. дис... канд. пед. наук: 13.00.04 / О.С. Куценко; Клас. приват. ун-т. — Запоріжжя, 2008.

16. Чусовитин Ю. Как убережть ребенка от виртуальной зависи-мости? [Електронний ресурс] / Ю. Чусовитин. — Електрон. дані. — Режим доступу : <http://shkolazhizni.ru/archive/0/n-24010/>. — Загол. з титулу екрану.

17. <http://osvita.ua/school/technol/6804>

18. <http://http/sputnikmedia.net/news/854/>

19. <http://uk.wikipedia.org/wiki/>

20. <http://ammvizeum.wordpress.com/2010/03/02/>

21. <http://www.dt.ua/3000/3855/65829/>

22. <http://www.eukidsonline.net/>

23. <http://www.microsoft.com/protect/parents/cyberethics/practice.aspx>.

Зміст

Передмова	3
I. Інформаційно-комунікаційні технології у сучасному навчальному закладі.....	5
II. Інтернет в Україні.....	7
1. Діти в Інтернеті. Дослідження з проблем використання Інтернету дітьми в Україні.....	8
2. Інтернет-можливості для розвитку дітей.....	10
3. Інтернет-загрози для дітей.....	12
III. Превентивна робота, спрямована на виховання культури та безпечної поведінки користувача Інтернету.....	19
1. Діяльність Коаліції за безпеку дітей в Інтернеті	19
2. Захист дітей та молоді від негативних інформаційних впливів – один із напрямів української державної політики в галузі освіти.....	22
3. Загальні методичні рекомендації. Формування у дітей компетенцій безпечного користування ресурсами мережі Інтернет.....	24
4. Підготовка педагогів-тренерів з безпеки в Інтернеті.....	29
4.1. Загальні методичні рекомендації.....	29
4.2. Структурно-логічна модель підготовки педагогів-тренерів з безпеки в Інтернеті.....	33
5. Організація навчально-виховної роботи з дітьми 7-10 років.....	37
5.1. Вікові психофізіологічні особливості.....	37
5.2. Формування у дітей навичок критичного мислення.....	39
5.3. Структурно-логічна модель тренінгу для дітей 7-10 років з безпеки в Інтернеті.....	42
6. Організація навчально-виховної роботи з дітьми 11-18 років.....	45
6.1. Врахування психологічних особливостей дітей при організації тренінгів.....	45
6.2. Використання навичок критичного мислення при оцінюванні Інтернет-ресурсів	48
6.3. Структурно-логічна модель тренінгу для дітей 11-18 років з безпеки в Інтернеті.....	51
IV. Відповідальність батьків за безпеку дітей в Інтернеті. Рекомендації для педагогів з питань організації превентивної роботи з батьками.....	54
Додатки.....	61
Література.....	97

«Виховання культури користувача Інтернету. Безпека у всесвітній мережі»: навчально-методичний посібник /
А.Б. Кочарян, Н.І. Гущина. - Київ, 2011. – 100 с.

Рецензенти:

В.М. Оржеховська

Н.А. Саражинська

Упорядники: *Я.А.Курченко, А.Б.Кочарян*

Відповідальна за випуск *Пушкарьова Т.О.*

Редактор *Бігун Н.М.*

Комп'ютерна верстка *Громська О. І.*