***Практичний психолог студентам***

**Інтернет загрози та безпека в Інтернеті**

Інтернет-технології стали природною, невід’ємною частиною життя сучасних людей і особливо дітей та молоді. Невміння працювати з комп’ютером і орієнтуватися в інтернет-просторі в сучасному суспільстві можна порівняти з невмінням писати й читати. Комп'ютер є не тільки розвагою, але й засобом спілкування, самовираження та розвитку. У кіберпросторі існує велика кількість спеціальних сайтів, адресованих людям різного віку. Самостійне пізнання інформаційного світу дозволяє розширити коло інтересів людини , сприяє її додатковій освіті, спонукає до кмітливості, привчає до самостійного розв'язання задач.

**Чим приваблює інтернет дітей і підлітків?**

* Різноманітне спілкування, знайомства і пошук нових друзів у соціальних мержах, чатах, участь у дискусіях і віртуальних форумах.
* Утамування інформаційного голоду.
* Навчання і розвиток – контрольні, реферати і курсові роботи, новини, підвищення рівня знань, технічної і медійної освіченості.
* Розваги – ігри, прослуховування музики, перегляд фільмів і відео.
* Пошук нових форм самовираження.
* Анонімність і віртуальна свобода (моделювання множинності «Я»).
* Відчуття спільності та приналежності до групи.

Всесвітня мережа також задовольняє потребу підлітків у лідерстві. Діти, які добре знають комп'ютер та інтернет більш адекватно оцінюють свої здібності та можливості, вони більш цілеспрямовані та кмітливі .

Щоб повноцінно орієнтуватись у віртуальному просторі людині треба вчитися структурувати великі потоки інформації, дотримуючись основних правил безпеки в Мережі.

Завданням, як дорослих, так і дітей, і підлітків – навчитися правильно та безпечно користуватися Інтернетом. Так само, як ми вчимося безпеки в реальному житті - на вулиці та дорозі, нам необхідно навчитися безпечній поведінці у віртуальному житті - в Інтернеті.

**ІНТЕРНЕТ ЗАГРОЗИ**

**1 Комп’ютерна залежність.**

До комп’ютерної залежності більш схильні підлітки 11-17 років. У них відбувається втрата відчуття часу, порушення зв’язків із навколишнім світом, виникає почуття невпевненості, безпорадності, страху самостійного прийняття рішеннь і відповідальності за них. Комп’ютерна залежність негативно впливає на особистість дитини, викликаючи емоційну й нервову напругу, астеноневротичні та психоемоційні порушення, проблеми у спілкуванні та порушення соціальної адаптації. Нічне використання Інтернету спричиняє порушення режиму сну, внаслідок чого виникає хронічна втома, підвищується дратівливість, конфліктність. З метою подолання сонливості діти, які страждають залежністю, вдаються до підвищеного споживання кави, міцного чаю та інших тонізуючих речовин, що також шкодить їх здоров’ю. Щоб придбати нові ігри чи пристрої для гри або для оплати користування інтернетом деякі діти вдаються до шахрайства. За ступінню впливу на гравця найбільш потужними є рольові комп’ютерні ігри, які сприяють інтеграції свідомості з комп’ютером, що може призвести до повного самоототожнення дитини з комп’ютерним героєм. У нормальному стані відбувається короткочасове поринання гравця у віртуальну реальність з метою зняття напруги, відволікання від побутових проблем. У випадку патологічного відхилення від норми, дитина повертається у реальний світ на короткий проміжок часу, тільки щоб поїсти, попити і трохи поспати. Перебування залежної дитини в кіберпросторі може сягати 18 годин на добу. Залежність, як правило, помічають рідні і близькі користувача за змінами у поведінці, інтересах і режимі дня.

**Психологічні і фізичні симптоми інтернет залежності.**

**Психологічні симптоми:**

* гарне самопочуття або ейфорія під час роботи за комп’ютером; неможливість зупинитися;
* постійне збільшення кількості часу перебування в інтернеті;
* зневага родиною і друзями;
* відчуття спустошіння, тривоги, роздратуванності в періоди перебування поза інтернетом;
* брехня про свою діяльність своїм близьким;
* проблеми з навчанням.

**Фізичні симптоми:**

* біль в області зап’ястя через тривалу перенапругу м’язів;
* сухість в очах;
* головний біль;
* більуспині;
* нерегулярне харчування;
* зневага особистою гігієною;
* порушення сну.

**Небезпечні сигнали, передвісники інтернет залежності:**

* нав’язливе прагнення постійно перевіряти електронну пошту;
* очікування чергового сеансу онлайн;
* збільшення часу, проведеного онлайн;
* зростання витрат на інтернет-послуги.

**Ознаками інтернет залежності є:**

* повне поглинання інтернетом;
* потреба у збільшенні часу онлайн-сеансів;
* наявність неодноразових, малоефективних спроб скорочення часу перебування в інтернеті;
* поява симптомів абстиненції при скороченні користування інтернетом (повторна тяга, виникнення і посилення напруги через певний час);
* виникнення проблем з оточуючим середовищем (однолітками,членами родини, друзями);
* намагання приховати реальний час перебування в інтернеті;
* залежність настрою від використання інтернету (виражається емоційним і руховим збудженням, тривогою, нав’язливими розмірковуваннями про те, що зараз відбувається в інтернеті, фантазіями і мріями про інтернет, вільними чи несвідомими рухами пальців, що нагадує друкування на клавіатурі).

**2 Розходження між реальним «Я» і своїм інтернет образом** може бути наслідком неадекватного сприйняття підлітком себе і оточуючого світу. Ототожнюючи себе з героєм гри, гравець отримує можливість своєрідної самореалізації у віртуальному світі. При цьому якості героя (сміливість, сила, надзвичайні здібності та ін.) він автоматично приміряє на себе. Повернення в реальність позбавляє гравця багатьох можливостей і робить безпорадним перед проблемами, що існують в реальності. Це призводить до погіршення психологічного стану: зміни емоційного стану, підвищення тривоги, роздратованності, зниження самооцінки, проявів невпевненності в собі, виникнення агресії до оточуючих, погіршення навчальних показників і порушення соціалізації.

**Існують часові норми перебування за комп’ютеромдля дітей різного віку:**

Згідно з нормами, визначеними Міністерством охорони здоров’я України, безперервне перебування за комп’ютером в продавж доби не повинно перевищувати: 1-2 клас – 10 хв. 3-5 клас – 15 хв. 6-7 клас – 20 хв. 8-11 клас – 30 хв. Для дітей 1 класу загальний час використання комп’ютера з рідкокри- сталічним монітором має обмежуватися 30-45 хвилинами на тиждень,

2-3 класів – 2 години на тиждень, але не більше 1 години на добу,

4-6 класів – 2 години на тиждень, але не більше 1 години на добу,

7-9 класів – 2,5 години на тиждень, але не більше 1 години на добу

і учнів 10-11 класів – 7 годин на тиждень, але не більше 1 години на добу.

**3 Доступ до небажаного контенту** (матеріалам непридатного для дітей та протизаконного змісту – порнографічним, тим що пропагують наркотики, психотропні речовини й алкоголь, тероризм і екстримізм, ксенофобію, сектантство, національну, класову, соціальну нетерпимість і нерівність, асоціальну поведінку, насилля, агресію, суїцид, азартні ігри, інтернет-шахрайство, та матеріалам, що містять образи, наклепи і неналежну рекламу).

Небезпека перегляду ресурсів з «дорослим» контентом полягає у тому, що, по-перше, ви можете бути ще емоційно не готовими до сприйняття відвертих матеріалів, що стосуються статевих відносин, та можуть завадити формуванню нормальної сексуальної та громадської поведінки, справити негативний вплив на уяву про здорові сексуальні стосунки, нівелювати сімейні цінності та сприяти ранньому початку інтимного життя;

по-друге - можете стати жертвою злочинців, педофілів чи людей з порушенням психіки.

Перегляд матеріалів, що містять сцени насилля та жорстокості щодо людей і тварин, що пропагують протиправну і антисуспільну діяльність - перешкоджає нормальному формуванню моральних цінностей.

**4 Розкриття конфіденційної інформаціїу Мережі** – це повідомлення повного власного імені чи імен членів родини, адреси проживання і навчального закладу, номерів телефонів, місця відпочинку, часу повернення додому, періоду відсутності батьків чи інших членів родини, номерів банківських карток батьків чи інтернет-гаманця, повідомлення паролей до електронної пошти та акаунтів соціальних мереж.

При реєстрації в інтернет-сервісах у кодових фразах не слід повідомляти свідчення особистого характеру, наприклад, дівоче прізвище матері, оскільки дана інформація використовується при оформленні банківських документів у якості ключової фрази. Іноді дорослі самі розповсюджують через соціальні мережі та форуми інформацію про себе і своїх дітей, включаючи розміщення фотокарток родини, інформації про місце роботи і час повернення додому, місця відпочинку і точні дати відсутності. Це може зацікавити злочинців та поставити під загрозу безпеку дитини. Фотокартки, що розміщуються вами на персональній сторінці, але закриті для загального доступу, все рівно можуть потрапити на інші сервіси, де стануть загальнодоступними. Нерідко підлітки, які перебувають у романтичних стосунках вимагають одне від одного паролі до комунікаційних сервісів. При цьому дівчата більш схильні до розголошення власних даних.

**5 Надмірна зацікавленість індивідуальними та, або мережевими онлайн- іграми.** Агресивні ігри з деструктивним змістом, що закликають до насилля і руйнування. Такі ігри негативно впливають на психіку дитини, підвищують тривожність і дратівливість, роблять її більш збудженою і неслухняною, вчать вирішувати проблеми з позиції сили. Конфлікти, що виникають між гравцями, можуть призвести до драматичних наслідків у результаті з’ясування стосунків у реальності.

**6 Надмірне ахоплення азартними мережевими іграми, віртуальними казино (онлайн-гембілнг)**

**7 Кібероніоманія.** Неконтрольовані покупки в інтернет-магазинах, без не- обхідності їх придбання та урахування власних фінансових можливостей, по- стійна участь в онлайн-аукціонах.

**8 Кіберкомунікативна залежність** (надмірне спілкування у чатах, участь у телеконференціях).

**9 Кіберсексуальна залежність** (нездоланний потяг до обговорення сексуальних тем на еротичних чатах і телеконференціях, відвідування порнографічних сайтів і заняття кіберсексом). Перехід від віртуальних стосунків до реальних -залучення неповнолітніх до сексуальних стосунків;

-залучення через інтернет дітей і підлітків до протизаконної діяльності;

-знайомства через інтернет з метою пошуку сексуального партнера

**10 Секстинг** – новий вид розваг: фотографування себе у роздягненому виг- ляді на камеру телефона чи комп’ютера, з метою пересилки знімків друзям. Частіше за все секстинг використовують закохані пари, ті, хто хоче вихвали- тися перед знайомими романтичними стосунками або підлітки, які розрахо- вують на взаємність.

**11 Нав’язливий веб-серфінг,** блукання по Мережі, пошук у віддалених базах даних (відвідування сайтів новин, читання інформації на форумах, блогах, перегляд і прослуховування інформації в різних форматах).

Веб-серфінг затягує дитину, відволікаючи її від навчання та інших справ, оскільки, потрапивши в інформаційний потік, втрачається відчуття часу.

**12 Відвідування сайтів агресивної (**що пропагують ксенофобію, тероризм**) і аутоагресивної спрямованості** (кіберсуїцид, онлайн-суїцид, суїцидальні домовленності, інформаційні ресурси про застосування засобів для суїциду з описом їх дозування і вірогідності летального результату).

**13 Адиктивний фанатизм** (релігійний – сектантство, політичний – партійний, національний, спортивний, музикальний і т.ін.).

**14 Пристрасть до роботи з комп’ют**ером – програмування, хакерство. Основні мотиви хакерства: допитливість, боротьба за вільне розповсюдження і доступність інформації, самоствердження, відчуття власної сили, захоплення процесом, недостатність пізнавальної активності при навчанні, належність до «хакерскої культури», залежна поведінка.

**15 Гаджетадикція** (пристрасть до заволодіння конкретним мобільним обладнанням, приладом, що має вихід у інтернет: стільниковим телефоном, смартфоном, комунікатором, міні-комп’ютером, КПК і залежність від його використання).

**16 Кібербулінг** – одна з форм переслідування дітей і підлітків з використанням цифрових технологій. Іноді для цього створюються сайти, де розміщуються компрометуючі матеріали на дитину, яку переслідують. Якщо ж раптом Ви отримали численні електронні повідомлення агресивного змісту від незнайомців, якщо Вас почали переслідувати й залякувати, це означає, що Ви потрапили під кібербулінг.

**Для кібербулінгу використовуються:**

**-** мобільний зв’язок (використання фото і відео для дискредитації та залякування жертви, доставка текстових і мультимедійних повідомлень);

- сервіси миттєвих повідомлень (використання ICQ для відправки повідомлень, взламування акаунта із розісланням дискредитуючих повідомлень рідним і друзям жертви);

-електронна пошта(розсилання повідомлень і листів, що містять залякування, віруси,публікація в Мережі листів жертви особистогохарактеру);

- форуми і чати (розсилання агресивних повідомлень, розкриття анонімності акаунта жертви, розміщення на сторінках форуму інформації про жертву конфіденційного і особистого характеру);

- соціальні мережі (розміщення коментарів, що містять залякування і знущання, фото і відеоматеріалів,блокування акаунта жертви і розсилання масових скарг і претензій на володаря акаунта, створення акаунта від імені жертви з її подальшим використанням для дискредитації жертви);

-веб-камери (провокування жертви на відео запис з подальшою публікацією в інтернеті);

- сервіси відеохостингу (розміщення відеороликів, що містять знущання або залякування);

- ігрові сайти та віртуальні світи (розміщення повідомлень, що принижують і залякують жертву або шкодять її ігровому персонажу з метою психологічного тиску).

**17 Зіткнення з гриферами**. Інтернет-хулігани заважають гравцям (особливо початківцям) спокійно грати, постійно наносять пошкодження їхнім пер сонажам, блокуючи функції гри і створюючи неможливі умови для всієї команди Мережі, переслідуючи окремих її гравців.

**18 Кібергрумінг.** Входження в довіру дитини з метою використання її у сексуальних цілях. Злочинці добре розуміються на психології дітей і підлітків та орієнтуються в їхніх інтересах. Встановлюючи контакти в соціальній мережі або на форумах з дітьми, що знаходяться у пригніченому психологічному стані, вони співчувають, пропонують підтримку, обговорюють з дитиною питання, які її турбують, поступово переводячи їх у сексуальну площину, а потім пропонують перейти до стосунків у реальному світі. Виробництво, розповсюдження та зберігання дитячої порнографії. Слід пам’ятати, що незважаючи на згоду дитини на участь у порнографічних сесіях, відповідальність цілком покладається на дорослих. 20 січня 2010 року було прийнято Закон України №1819-VI «Про внесення змін до деяких законодавчих актів України щодо протидії розповсюдженню дитячої порнографії». Відповідно до статті 301 Кримінального кодексу України, виготовлення і розповсюдження порнографічної продукції або змушення неповнолітніх до участі у створенні зображень, відеопродукції або комп’ютерних програм порнографічного характеру карається позбавленням волі від п’яти до десяти років.

**19 Шахрайство в Мережі Інтернет**- чи мобільне шахрайство є способами здійснення злочину з використанням сучасних технологій. Відповідно до Кримінального кодексу України, шахрайство, в залежності від особливостей і складності здійсненого злочину карається позбавленням волі від трьох до дванадцяти років з конфіскацією майна. Також в Особливій частині Розділу ХVI є низка статтей, що передбачають покарання «за злочини в сфері використання електроннообчислювальних машин (комп’ютерів), систем і комп’ютер-них мереж електрозв’язку»

**ІНТЕРНЕТ ШАХРАЙСТВО:**

**Генерування кодів для карток оплати мобільного зв’язку.** Пропозиція програми генерування PIN-кодів для карток експрес-оплати за мобільний зв’язок. Запропонована програма виявляється генератором випадкових чисел. Налаштування безкоштовного використання послуг мобільного оператора.На безкоштовних хостингах розміщуються сайти-одноденки, працівники яких представляються співробітниками певного мобільного оператора та за певну суму пропонують повідомити налаштування для безкоштовного використання послуг.

**«Читай чужі SMS».** Пропозиція придбати спеціальну програму, що «дозволяє» читати SMS у чужому телефоні, переглядати адресну книгу та історії дзвінків.

**Продаж продукту, що неіснує** (програм, аудіофайлів, товарів, інформації).

**Прохання відправити SMS-повідомлення** для отримання коду виявляється звичайним виманюванням коштів. Зазвичай «неможливість відправити повідомлення» призводить до численного зняття коштів з рахунку абонента.

**«Передзвони мені».** Дзвінок з незнайомого номера з проханням зателефонувати. При спробі з’єднання з рахунку абонента знімаються кошти. **Фішинг –** технологія інтернет-шахрайства з метою крадіжки конфіденційної інформації (імен і паролей доступу, даних банківських карток і інтер нетгаманця й т.ін.).

**Поштовий фішинг** – отримання листа з вимогою повідомлення особистих даних.

**Онлайн-фішинг** – копіювання дизайну і доменних імен сайтів та інтернет-магазинів з метою обдурити покупця.

**Комбінований фішинг** – створення підробного сайту, де жертва самостійно заповнює форми, повідомляючи шахраям конфіденційні дані, або використання програм-шпигунів key-loggers, що фіксують інформацію, введену з клавіатури та пересилають її шахраям.

**Вішинг** – технологія інтернет-шахрайства з метою крадіжки конфіденційної інформації за допомогою інтернет-телефонії і автонабирачів. Абоненту пропонується зателефонувати за міським номером, де звучить повідомлення про необхідність надання особистої інформації.

**Фармінг** – перенаправлення трафіку із завантаженого веб-вузла на клон сайта, що хотів відвідати користувач. Далі відбувається зараження вірусами або активація файлу, що може пошкодити комп’ютер.

**Пам’ятка щодо безпеки в Інтернеті:**

1 Важливість захисту своєї та чужої конфіденційної інформації:

• не можна викладати в інтернеті інформацію про сім'ю та її фінансові справи, адреси проживання та навчання, номери телефонів, коди кредитної картки та банківські дані;

• нікому, крім батьків, не можна називати власні паролі до інтернет-сервісів (навіть найкращим друзям).

2 Поводитися у Всесвітній Мережі потрібно так само, як і у реальному житті: ввічливо, не робити нічого, що може образити інших людей або суперечить закону.

3 В Інтернеті також слід із повагою ставитися до людей та їх авторських прав. Незаконне копіювання та розповсюдження матеріалів, що є чиєюсь власністю, вважається крадіжкою.

4 Віртуальний співрозмовник може видавати себе за іншого. Не надто довіряйте незнайомим людям у Мережі.

5 Віртуальний світ іноді коштує реальних грошей. Завжди потрібно з'ясовувати, скільки коштують спеціальні інтернет-сервіси: наприклад, якою є повна вартість SMS в онлайн-грі, скільки насправді коштують такі SMS- послуги та чи дійсно необхідно їх надсилати.

6 Необхідно звертатися за порадою до близької людини, якщо в Інтернеті (у повідомленні електронної пошти, на сайті, форумі, чаті) щось не зрозуміло, хвилює або загрожує.

7 Інформація та послуги в Інтернеті не завжди безпечні, тому перш ніж завантажувати, копіювати чи встановлювати будь-що з Інтернету, перевіряйте інформацію за допомогою додаткових запитів і звернення до перевірених джерел.

«ГАРЯЧІ» КОНТАКТИ З ІНТЕРНЕТ БЕЗПЕКИ

1Спеціальний розділ сайту компанії«Київстар» із захисту дітей від негатив- ного контенту. Проконсультуватися з експертом з онлайн-безпеки можна на сайті http://online-bezpeka.kyivstar.ua, де кваліфіковані спеціалісти дадуть відповіді на Ваші питання.

2Електронна гаряча лінія з протидії дитячої порнографії в інтернеті«Ла Страда-Україна». Повідомити про випадки дитячої порнографії в інтернеті можна за допомогою форми на головній сторінці www.internetbezpeka.org.ua Головною метою роботи ресурсу є блокування розповсюдження дитячої пор- нографії, особливо на серверах українських інтернет-провайдерів. Гаряча лінія функціонує на базі Міжнародного жіночого правозахисного центру «Ла Страда-Україна».

3 Національна «гаряча лінія» з питань протидії домашньому насильству і захисту прав дітей.

Звернувшись на гарячу лінію за телефоном 0 800 500 335 (безкоштовно для дзвінків із стаціонарних телефонів на території України), або 386 (безкоштовно для дзвінків з телефонів мобільних операторів «Київстар» і «МТС») чи електронною поштою на info@lastrada.org.ua, onlandia@live.com, можна одержати такі консультації:

• Правила безпечної поведінки дітей під час користування інтернетом.

• Поради батькам з безпечної роботи дітей в інтернеті.

• Попередження комп’ютерноїзалежності і можливість отримання психологічної допомоги. • Юридичні консультації стосовно злочинів проти дітей в інтернеті.

• Допомога у випадках або підозрах загрози дітям через інтернет.

Гаряча лінія працює на базі Міжнародного жіночого правозахисного центру «Ла Страда-Україна» за інформаційної підтримки проекту «Онляндія».

4. Проект із протидії незаконним матеріалам в інтернет-просторі України Skarga.ua Кожний користувач українських інтернет-порталів може сповістити про матеріали, що порушують законодавство країни та містять порнографію з участю неповнолітніх, прояви расової і національної нетерплячості, вияви тероризму, заклики до насильницької зміни конституційного ладу за допомогою форми на головній сторінці http://skarga.ua/ Проект створений Інтернет-Асоціацією України.

5.Телефон Довіри МВС України Телефон довіри Департаменту МВС: (+380 44) 254-76-04. Повідомити про веб-сайти, що пропагують насильство і жорстокість або розпалюють ненависть, расову дискримінацію, займаються створенням чи розповсюдженням дитячої порнографії можна в Департамент боротьби зі злочинами, пов’язаними з торгівлею людьми МВС України.

***За матеріалами Посібника для батьків «Діти в Інтернеті: як навчити безпеці у віртуальному світі» Ігор Володимирович Литовченко, Сергій Дмитрович Максименко,Сергій Іванович Болтівець, Мирослав-Любомир Андрійович Чепа, Наталія Михайлівна Бугайова. – К.: Видавництво: ТОВ «Видавничий Будинок“Аванпост-Прим”,2010. – с. –48.***