Відділ освіти Срібнянської районної державної адміністрації
Районний методичний кабінет

ЗАХИСТ ДІТЕЙ ВІД ШКІДЛИВОГО ВПЛИВУ МЕРЕЖІ ІНТЕРНЕТ

Навчально-методичний посібник.

Срібне
2015

Захист дітей від шкідливого впливу мережі Інтернет: навчально-методичний посібник. – Срібне, 2015, 25 с.

Навчально-методичний посібник розглянутий на Раді РМК відділу освіти Срібнянської районної державної адміністрації та рекомендований для використання в роботі (протокол № 3 від 24.12.2015 року).

Рецензент: Мотузка Людмила Іванівна, завідувач РМК відділу освіти Срібнянської районної державної адміністрації.

Автор-укладач – Шпитяк Віталій Анатолійович, методист районного методичного кабінету відділу освіти Срібнянської районної державної адміністрації

У навчально-методичному посібнику містяться відомості про можливості та загрози глобальної мережі Інтернет, а також загальні рекомендації для вчителів і батьків щодо використання програмних засобів для захисту дітей від шкідливого впливу мережі Інтернет.

Відповідальний за випуск: Шпитяк Віталій Анатолійович, методист районного методичного кабінету відділу освіти Срібнянської районної державної адміністрації

Навчально-методичний посібник надруковано в РМК відділу освіти Срібнянської районної державної адміністрації

Зміст

Вступ

Інформаційно-комунікаційні технології (ІКТ) – це технології, призначені для створення, опрацювання, збереження, передачі та управління інформацією. Цей термін охоплює в собі 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. На сьогодні інформаційно-комунікаційні технології включають апаратні засоби (комп'ютери, сервери, мережеві пристрої) та програмні (операційні системи, мережеві протоколи, пошукові системи тощо).

У сучасному світі ІКТ є важливою і невід'ємною частиною життя держави, бізнесу та приватного життя. Згідно статистики, кожні 72 години кількість інформації збільшується вдвоє, тому потрібні спеціальні навички та вміння для опрацювання такого величезного інформаційного об'єму.

Якщо раніше головним джерелом інформації і знань вважалася книга, то в XXI столітті діти з раннього віку вже знайомі з комп'ютерами, мобільними телефонами, телебаченням, тощо. Все це безумовно впливає на розвиток дитини, змінює її внутрішній світ, способи сприйняття та участі в оточуючому світі. Подача та отримання інформації за допомогою ІКТ є вже звичною і зрозумілою для дитини реальністю. Великі можливості для реалізації інформаційних процесів надає глобальна мережа Інтернет.

На сьогодні Інтернет є найбільш популярним технологічним винаходом у світі. За даними звіту Міжнародного союзу електрозв'язку (МСЕ) на кінець 2014 року в світі налічувалося до 3 млрд. користувачів глобальної мережі. В Україні за статистикою в 2014 році експерти налічували 18,5 млн. користувачів (41,2 %) і їх кількість постійно зростає.

Інтернет відкриває безмежні можливості, але разом з тим передбачає велику відповідальність. Безпека дітей в Інтернеті вже довгий час є актуальною темою в багатьох країнах світу. В Україні це питання також набуває дедалі більшої актуальності. Знання загроз, які існують в глобальній мережі та засобів захисту від них дозволить безпечно користуватися Інтернетом та розкрити всі можливості, які він дарує.

Розділ І. Інтернет і розвиток сучасної дитини

Глобальна мережа Інтернет на сьогодні є однією з найбільш популярних інформаційно-комунікаційних технологій. І дорослі і діти використовують її з різною метою – для роботи та пошуку інформації, для спілкування, для розваг. Щороку в Україні кількість користувачів Інтернету зростає, в тому числі дедалі більше дітей та підлітків отримують доступ до мережі. Із зростанням кількості користувачів поступово поліпшується і якість надання послуг доступу до Інтернету, що безумовно розширює можливості з використання її служб і сервісів.

Найпопулярнішими службами мережі Інтернет на сьогодні є такі:

1. **Всесвітня мережа** (англ. World Wide Web, скорочено: WWW) – найбільше всесвітнє багатомовне сховище інформації в електронному вигляді: десятки мільйонів пов'язаних між собою документів, що розташовані на комп'ютерах, розміщених на всій земній кулі. Вважається найпопулярнішою і найцікавішою службою мережі Інтернет, яка дозволяє отримувати доступ до інформації незалежно від місця її розташування.

   У всесвітній мережі знаходиться більше 1 мільярда веб-сайтів, кожен з яких - сукупність веб-сторінок, що об'єднані як за змістом, так і за навігацією.

   Кожен веб-сайт складається як мінімум з 1 і більше веб-сторінок, ніби книга. Та на відміну від звичайних книг, сайти мають **«гіперпосилання»** – фрагменти тексту чи зображень, натискання на які призводить до переходу на іншу веб-сторінку цього ж сайту або будь-якого іншого. Кожен сайт в мережі має свою унікальну адресу, (наприклад osvita-sribne.tk).

   Переходячи за гіперпосиланнями з сайту на сайт, користувачі подорожують всесвітньою мережею в пошуках корисної інформації чи з метою відпочинку, здійснюють покупки, спілкуються тощо.

   Знаходити потрібну інформацію серед такого величезного інформаційного об’єму допомагають **пошукові системи** (www.google.com, www.meta.ua).

   На сьогодні в молоді користуються популярністю **соціальні мережі** – сайти, на яких можна створювати спільноти, власні сторінки з

інформацією про себе, розміщувати фото, аудіо- та відеоматеріали, обмінюватися миттєвими повідомленнями та слідкувати за оновленнями на сторінках друзів.

2. **Електронна пошта** (англ. e-mail) – популярний сервіс в Інтернеті, що робить можливим обмін даними будь-якого змісту (текстові документи, аудіо-, відео-файли, архіви, програми). На поштових серверах кожен може безкоштовно створити свою електронну поштову скриньку, яка має унікальну адресу і ідентифікує власника. Наприклад, osvita-sribne@ukr.net, де **osvita-sribne** – це нікнейм (ім'я) власника, а **ukr.net** – поштовий сервер, що надає послугу з електронного листування. Між цими частинами адреси знаходиться символ **@** (собака, мавпа, равлик).
3. **IRC** (англ. Internet Relay Chat) – сервіс Інтернет, який надає користувачам можливість спілкування шляхом надсилання текстових повідомлень багатьом людям з усього світу одночасно (в режимі реального часу). Кожен користувач «чату» має свій «нікнейм» – ім'я, яке ідентифікує його (зазвичай вигадане або похідне від справжнього).
4. **Аудіо- та відео конференції** – сервіси Інтернету для миттєвого обміну аудіо- та відеоінформацією в режимі реального часу.
5. **FTP** – сервіс прийому і передачі файлів через мережу Інтернет з одного комп'ютера на інший.
6. **Онлайн-ігри** – це комп'ютерні ігри, в яких учасникам ігрового процесу протистоїть не штучний інтелект, а такі ж реальні гравці, об'єднанні в віртуальному ігровому середовищі за допомогою глобальної мережі.

Розділ ІІ. Інтернет-загрози

Глобальна мережа Інтернет відкриває нові можливості в сфері інформаційно-комунікаційних технологій, забезпечує швидкий доступ до інформації, дозволяє реалізовувати фактично миттєвий, в режимі реального часу, обмін повідомленнями, дозволяє цікаво проводити дозвілля тощо. У віртуальному просторі діти та підлітки прагнуть дізнатися щось цікаве і корисне, прагнуть абстрагуватися від власних психологічних проблем. Віртуальний світ дозволяє дітям реалізувати цілу низку базових потреб: спілкування, ігри, розваги, саморозвиток та самореалізація, виховання сміливості, вміння долати перешкоди.

Але разом з тим, в Інтернеті приховано дуже багато небезпек, як для дітей, так і для дорослих. Знання цих небезпек дозволить їх уникнути.

2.1. Інтернет-залежність

Інтернет-залежність є складовою комп'ютерної залежності і полягає в надмірному користуванні ІКТ, проведенні великої кількості часу в Інтернеті. До комп'ютерної залежності більше схильні підлітки 11-17 років. У них відбувається втрата відчуття часу, порушення зв'язків з навколишнім світом, виникає почуття невпевненості та безпорадності, страху самостійно приймати рішення та відповідати за них.

Комп'ютерна залежність негативно впливає на особистість дитини, викликаючи емоційну та нервову напругу, астеноневротичні та психоемоційні порушення, проблеми у спілкуванні та порушення соціалізації.

Особливо шкідливими елементами комп'ютерної залежності є нічне використання Інтернету та рольові он-лайн-ігри. Виявити комп'ютерну залежність можна шляхом спостереження на основі ряду ознак:

- повне поглинання Інтернетом;
- потреба у збільшенні часу он-лайн-сеансів;
- наявність неодноразових, малоефективних спроб скорочення часу перебування в Інтернеті;
- поява симптомів абстиненції при скороченні користування Інтернетом (повторний потяг, виникнення й посилення напруги);
- виникнення проблем у навколишньому соціальному середовищі;

- намагання приховати реальний час перебування в Інтернеті;
- залежність настрою від використання Інтернету.

2.2. Комп'ютерні віруси

Комп'ютерний вірус – це невелика програма, яка здатна до саморозмноження й виконання різних деструктивних дій. На сьогоднішній день відомо понад 50 тис. вірусів і їх кількість постійно збільшується. Дія вірусів може проявлятися по-різному: від візуальних ефектів, що заважають працювати до повної втрати інформації. Значна кількість вірусів намагається приховати свою присутність на зараженому комп'ютері, займаючись викраденням конфіденційної інформації або розпочинаючи дію по команді зловмисника, що контролює вірусну програму.

Основними джерелами розповсюдження вірусів є:

- дискета або флеш пам'ять («флешка»);
- комп'ютерна мережа (локальна або глобальна);
- жорсткий диск, на який потрапив вірус;
- піратське програмне забезпечення.

Ознаки зараження вірусом:

- зменшення обсягу вільної оперативної пам'яті;
- уповільнення роботи комп'ютера, завантаження операційної системи;
- незрозумілі зміни у файловій системі (поява, зникнення чи зміна файлів і папок без участі користувача та операційної системи);
- неможливість зберігання файлів;
- помилки при роботі операційної системи та програм;
- незрозумілі системні повідомлення, звукові та візуальні ефекти.

2.3. Доступ до небажаного контенту

Під небажаним контентом розуміються матеріали непридатного для дітей та протизаконного змісту: порнографічні, такі що пропагують наркотики, психотропні речовини й алкоголь, тероризм і екстремізм, ксенофобію, сектантство, національну, класову й соціальну нетерпимість і нерівність, асоціальну поведінку, насилля, агресію, суїцид, азартні ігри, інтернет-шахрайство та матеріали, що містять образи, наклепи та неналежну рекламу.

Контент для дорослих

У Інтернеті дитина може легко отримати доступ до порноконтенту, набравши ключові слова в пошуковій системі. Навіть якщо дитина не шукала таких ресурсів, у ряді випадків вона може зіткнутися з цим контентом, перейшовши по фальшивому гіперпосиланні на якомусь із сайтів.

Пропагування сексуального насилля над дітьми, жорстокої поведінки, шкідливих звичок тощо

Перегляд матеріалів такого характеру перешкоджає нормальному формуванню моральних цінностей та може завдати психологічних травм.

Небезпека перегляду ресурсів з таким контентом дуже велика для психічного і фізичного здоров'я дитини, а різні інтернет-шахраї можуть завдати ще й матеріальної шкоди. Щоб цього не сталося, варто ознайомитися з видами інтернет-технологій, направлених завдавати шкоду користувачам мережі, в першу чергу дітям.

2.4. Он-лайн звaблення дітей

Злочинці за допомогою мережі Інтернет та завдяки анонімності намагаються завоювати довіру дитини з метою сексуального насилля.

2.5. Кібер-хуліганство

Кібер-хуліганство, на відміну від звичайного хуліганства, відбувається з використанням ІКТ, і полягає в інформаційній атаці на людину. Варіантів кібер-хуліганства досить багато:

1) Кібербулінг – переслідування особи з використанням сучасних електронних технологій та інших засобів електронної техніки.
2) Кібергрумінг – входження в довіру дитини з метою використання її в сексуальних цілях.
3) Грифери – інтернет-шахраї, які заважають учасникам он-лайн ігор спокійно грати. Вони пошкоджують віртуальних персонажів, викрадають їх, блокують функції гри тощо.
4) Тро́лінг (від англ. trolling) — розміщення в Інтернеті (на форумах, у групах новин Usenet, у вікі-проектах та ін.) провокаційних повідомлень з метою викликати флейм, конфлікти між учасниками, образи, війну редагувань, марнослів'я тощо. Тролінг є грубим порушенням мережевого етикету (нетикету).

2.6. Інтернет-шахрайство

Інтернет- чи мобільне шахрайство – є способом здійснення злочину за допомогою сучасних технологій. Існує велика кількість різновидів інтернет-шахрайства:

1) Фíшинг – вид шахрайства, метою якого є виманювання у довірливих або неуважних користувачів мережі персональних даних клієнтів онлайнових аукціонів, сервісів з переказування або обміну валюти, інтернет-магазинів. Шахраї використовують усілякі способи, які найчастіше змушують користувачів самостійно розкрити конфіденційні дані – наприклад, посилаючи електронні листи із пропозиціями підтвердити реєстрацію облікового запису, що містять посилання на веб-сайт в Інтернеті, зовнішній вигляд якого повністю копіює дизайн відомих ресурсів.
2) 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 надати конфіденційну інформацію.
3) Фармінг – перенаправлення жертви із завантаженого веб-узла на клон сайта, який хотів відвідати користувач. Далі відбувається зараження вірусами комп’ютера і/або крадіжка персональних даних.
4) Мобільне шахрайство – на мобільний телефон потенційної жертви зловмисник надсилає повідомлення різного змісту з проханням відправити СМС на вказаний номер, або поповнити рахунок тощо. Також шахраї можуть телефонувати і представлятися співробітниками банків, правоохоронних органів тощо і вводять в оману людину, змушуючи її перевести кошти на рахунок зловмисника.

2.7. Інші небезпечні загрози мережі Інтернет

Недостовірна інформація

У Інтернеті фактично відсутня будь-яка цензура, тому достовірність інформації теж не завжди відповідає дійсності, а часто й суперечить їй. Користування інтернет-джерелами завжди вимагає критичного ставлення до них, потрібно звірюватися з авторитетними джерелами інформації.

Спам

Спам – це масова розсилка рекламних або фішингових повідомлень власникам електронних поштових скриньок.

Розкриття конфіденційних даних

Повідомлення в мережі Інтернет 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 чи номерів інтернет-гаманця, повідомлення паролів від облікових записів на веб-сайтах може призвести до негативних наслідків, якщо ці дані потраплять до рук шахраїв.

Кібероніманія

Неконтрольовані покупки в інтернет-магазинах, без необхідності їх придбання та урахування власних фінансових можливостей, постійна участь в онлайн-аукціонах.

Кіберкомунікативна залежність

Надмірне спілкування у чатах, соціальних мережах тощо.

Кіберсексуальна залежність

Нездоланний потяг до обговорення сексуальних тем на еротичних чатах і телеконференціях, відвідування порнографічних сайтів і заняття кіберсексом.

Секстинг

Вид розваг, який передбачає фотографування себе у роздягненому вигляді на камеру телефону чи комп’ютера, з метою пересилки знімків друзям.

Розділ ІІІ. Технічні засоби захисту в Інтернеті

3.1. Способи Інтернет-цензури

Інтернет не перебуває під одноосібним керуванням якої-небудь держави, його ресурси розподілені між безліччю комерційних організацій, тому комплексна Інтернет-цензура достатньо складна. Вона можлива сукупним використанням наступних заходів:

1) Зосередження в руках держави управління мережевими комунікаціями або реальних важелів впливу на компанії, у віданні яких перебувають мережі, що виходять за межі держави. Це дозволяє директивним шляхом заборонити перегляд користувачами ресурсів, вміст яких вважається небажаним.
2) Постановка можливості доступу до Інтернет-ресурсів, контрольованим компаніями, в залежність від готовності таких компаній контролювати вміст ресурсів, видаляючи або редагуючи повідомлення, так чи інакше підпадають під цензуру влади країни. У результаті компанії, що підтримують, наприклад, систему мережевих блогів, опиняються перед вибором: або піддатися на шантаж та цензурувати інформацію, або відмовитися і втратити користувачів.
3) Також уряди мають можливість контролювати зміст деяких Інтернет-ресурсів через підставні фірми, «неурядові організації» або приватних осіб, які під різними приводами цензурують інформацію.

Крім випадків тотального контролю над стиком національних мереж із світовими в деяких країнах, таких як Китай, Північна Корея, Іран та ін., технічно важко зусиллями однієї держави подолати розподілену структуру Інтернету. Введення одних заходів веде до породження нових шляхів обходу обмежень. Найчастіше застосування цензури в Інтернеті більш затратно, ніж її подолання. Але величезні ресурси держав у багатьох випадках дозволяють її здійснювати.

В Україні відсутній тотальний контроль Інтернету, тому користувачі можуть подорожувати всесвітньою павутиною фактично без обмежень, що з одного боку виражає демократичність і толерантність в цьому питанні з боку держави, а з іншого – супроводжується високими ризиками потрапити на

ресурси з небезпечним контентом, ризиком зараження комп'ютера вірусами, широкими можливостями для інтернет-шахраїв. Щоб цього не сталося, користувачі комп'ютера повинні захистити себе і своїх дітей самостійно. Зробити це можна налаштувавши операційну систему, встановивши спеціальне програмне забезпечення для зменшення ризику наразитися на небезпечні явища в глобальній мережі.

Налаштування операційної системи і встановлення спеціального програмного забезпечення на локальному комп'ютері користувача може в більшості випадків вирішити проблему вільного доступу до сайтів із шкідливим контентом та захистити від вірусів. Тому це потрібно робити для зменшення ризиків зазнати негативного впливу мережі Інтернет, як в навчальному закладі, так і на домашньому комп'ютері. Адже обійти програмний захист зможе не кожна дитина, до того ж знизиться можливість випадкового потрапляння на шкідливі ресурси, знизиться імовірність зараження комп'ютера шкідливими програмами.

3.2. Захист комп'ютера та даних

Безпека комп'ютера – одне з першочергових завдань кожного користувача. Вірусні програми та хакерські атаки можуть спричинити серйозні моральні та матеріальні збитки – від викрадення та знищення інформації до програмного і технічного пошкодження ЕОМ. У більшості випадків захистити комп'ютер від вірусів та інших загроз не складно, але слід ставитися до цього ретельно і дотримуватися таких правил:

- Використовувати ліцензійну операційну систему та регулярно оновлювати її;
- Використовувати антивірусну програму, регулярно оновлювати антивірусну базу та періодично сканувати жорсткий диск комп'ютера на наявність вірусів;
- Для перевірки на віруси використовувати антивірусні сканери різних розробників;
- Використовувати брандмауер;
- Робити копії важливих даних;
- Перед відкриттям завантажених файлів перевіряти їх антивірусною програмою;
- Не використовувати піратські програми;

- Перевіряти флеш пам'ять, диски та інші носії даних;
- Ігнорувати електронні листи від невідомих адресатів, та не запускати файлів програм, надісланих електронною поштою
- Не зберігати конфіденційні дані на комп’ютері в незахищеному вигляді.

Антивірусна програма (антивірус) – програма для знаходження і лікування програм, що заражені комп'ютерним вірусом, а також для запобігання зараження файлу вірусом (Avast Free Antivirus, Avira Free Antivirus, Eset NOD32 та ін.).

Брандмауер (мережевий екран, файрво́л) – програма чи пристрій, що здійснює захист комп'ютерних мереж від хакерських атак через Інтернет.

Операційні системи сімейства Windows (зокрема Windows XP, Windows Vista, Windows 7, Windows 8) мають в своєму складі інтегрований брандмауер. Але при бажанні користувач ПК може відключити його і встановити будь-який інший (Comodo Firewall, Online Armor Free, Jetico Personal Firewall та ін.).

На сьогодні ряд найбільш відомих розробників антивірусного програмного забезпечення, поряд з антивірусами, випускає комплексні програмні засоби, які включають в себе і антивірус, і брандмауер. Таким чином реалізується повноцінний захист в одній програмі (Avast Internet Security, ESET NOD32 Smart Security, COMODO Internet Security та ін.).

3.3. Обмеження доступу до сайтів з небезпечним контентом

Задля обмеження доступу дітей до сайтів з небезпечним контентом потрібно здійснити налаштування операційної системи, браузера та пошукових систем, брандмауера. При потребі – встановити програми батьківського контролю. Деякі інтернет-провайдери дають можливість налаштувати рівень доступу до різних категорій веб-сайтів, обравши відповідний тариф або активувавши послугу.

1) Налаштування операційної системи та веб-браузерів

Найпростішим і досить ефективним засобом блокування шкідливої інформації в Інтернеті являється використання DNS-фільтрів. **DNS-фільтр** – інтернет-сервіс контентної фільтрації веб-сайтів.

Найпопулярнішими сервісами в україномовному сегменті мережі Інтернет є **Google Public DNS** та **Яндекс.DNS** – фільтри популярних пошукових систем.

Для налаштування DNS-фільтрації не потрібно встановлювати додаткового програмного забезпечення – фільтрація відбувається на пошуковому сервері. Потрібно лише прописати відповідні DNS у налаштуваннях мережевого підключення персонального комп'ютера або комутатора (тоді фільтрація відбуватиметься для всіх пристроїв, підключених до нього).

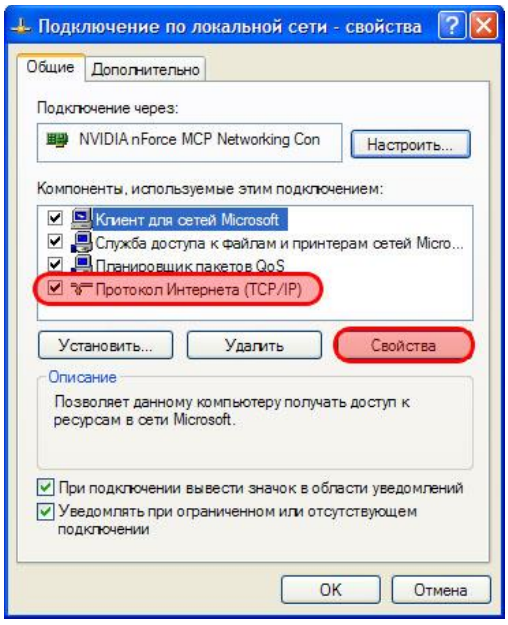
Приклад налаштування **Яндекс.DNS**
для операційної системи Windows XP

Сервіс Яндекс.DNS дає можливість обрати три режими:

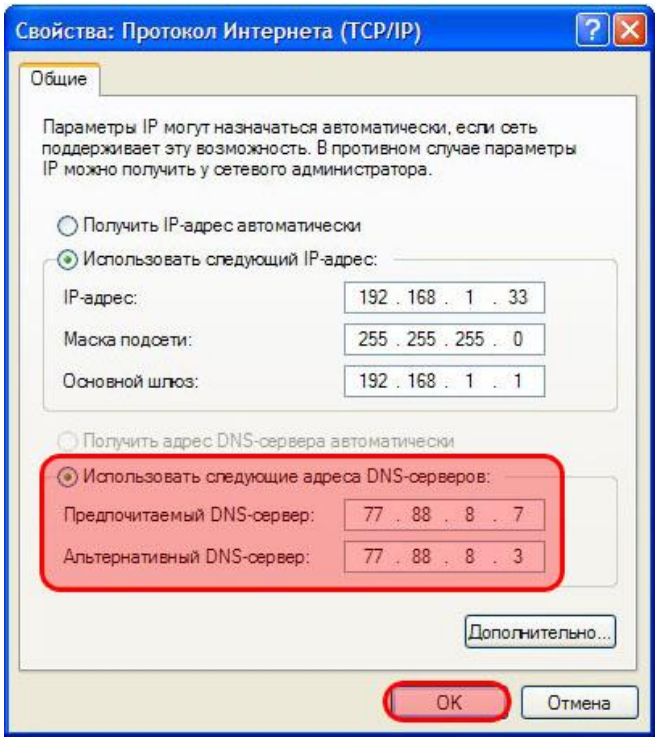
Базовий	**Безпечний**	**Родинний**
77.88.8.8 77.88.8.1	77.88.8.88 77.88.8.2	77.88.8.7 77.88.8.3
Швидкий та надійний DNS	Без шахрайських сайтів та вірусів	Без сайтів для дорослих

Відкриваємо меню **Пуск** → **Панель керування** → **Мережеві підключення.** Правою кнопкою миші викликаємо контекстне меню нашого мережевого підключення і обираємо пункт **Властивості** (Свойства).

У вкладці **Загальні** (Общие) знаходимо **Протокол Інтернету (TCP/IP)** (Протокол интернета (TCP/IP)) та відкриваємо його **Властивості** (Свойства).



Включаємо режим **Використовувати наступні адреси DNS-серверів** (Использовать следующие адреса DNS-серверов) і прописуємо адреси 77.88.8.7 та 77.88.8.3, потім зберігаємо налаштування натисканням кнопки **Ок**.



Відтепер при спробі знайти в Інтернеті шкідливу інформацію, вона буде відфільтровуватися DNS-серверами пошукової системи Яндекс.

Обхід захисту:

a) Зміна адрес DNS-серверів на комп'ютері або в налаштуваннях роутера.

Додатки (розширення) для браузера – програмне забезпечення, яке інтегрується в веб-браузер для розширення його функцій. Велика кількість необхідних додатків створена для браузера Mozilla Firefox. Але якщо на ПК встановлено декілька браузерів, то відповідний захист потрібно буде налаштовувати для кожного з них окремо, або видаляти зайві браузери.

Обхід захисту:

a) Використання альтернативних браузерів.
b) Відключення/видалення розширень.

2) Використання спеціальних комп'ютерних програм

Види комп'ютерних програм для захисту дітей в мережі Інтернет:

- **Програми батьківського контролю** – комплексне програмне забезпечення, що призначене для обмеження функцій персонального комп'ютера під час роботи за ним дитини (в тому числі і в Інтернеті).
- **Контент-фільтр (веб-фільтр)** – програмне забезпечення для фільтрації сайтів по їх змісту і/або по адресі сайту, доданого в «чорний список».
- **Брандмауер, мережевий екран** – програмне забезпечення, що здійснює контроль і фільтрацію мережевих пакетів відповідно до заданих правил.

Програми батьківського контролю обмежують доступ до аморальних або таких, що негативно впливають на опікувану особистість, інтернет-ресурсів. Але крім цього вони можуть виконувати ряд додаткових функцій: обмежувати загальний час використання ПК дитиною; визначати проміжки часу, в які дозволяється/забороняється працювати на комп'ютері; обмежувати доступ до програм та папок; записувати дії користувача ПК; створювати статистичні звіти тощо.

Принцип роботи веб-фільтрів полягає в наданні доступу до «білих» (корисних) і блокуванні «чорних» (шкідливих) сайтів, незалежно від того, яким браузером скористається дитина. Адміністратор комп'ютера може власноруч створювати і редагувати списки «білих» та «чорних» сайтів. Міру захисту теж можна обирати, переключаючи режими – від бездіяльності веб-фільтру до максимального захисту, в якому доступ буде надаватися лише до сайтів з білого списку. В режимі максимального захисту практично повністю реалізується обмеження доступу до шкідливих сайтів, але й велика частина корисних сайтів буде заблокована. Причиною цього є той факт, що сформувати повні списки корисних сайтів, так само як і повні списки шкідливих, ще нікому не вдавалося через їхню величезну кількість та динамічний розвиток інтернет-ресурсів.

Поряд з веб-фільтрами існують контент-фільтри. Вони так само намагаються блокувати шкідливі веб-сайти, але на відміну від перших, не на основі «білих» та «чорних» списків, а аналізуючи зміст веб-сторінки, до якої звертається користувач. Знайшовши недопустимий контент, програма блокує доступ до ресурсу. Проте й контент-фільтри мають недоліки – помилкове блокування корисних сайтів і в той же час пропуск шкідливого контенту.

Серед програм із вільною ліцензією слід відзначити веб-фільтр **«Інтернет Цензор»** (http://icensor.ru), програма проста в налаштуванні і досить ефективно забезпечує захист від сайтів із шкідливим контентом.

Zillya! Інтернет контроль (http://zillya.ua/zillya-internet-control) – українська програма для обмеження доступу до мережі Інтернет (по часу) та шкідливих сайтів, легко налаштовується та відносно якісно виконує свої функції.

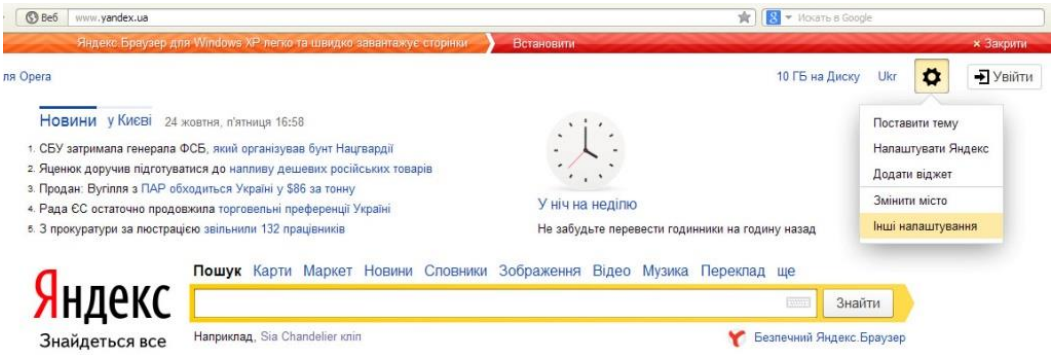
Такі програми при інсталяції зазвичай потребують введення паролю, який захищає програму від видалення та змін налаштування іншим користувачем (дитиною).

Обхід захисту:

a) У разі включення пошукових систем до «білих» списків веб-фільтру, за допомогою інструментів пошуку зображень та відео, користувач отримає доступ до небезпечного контенту на сторінках самої пошукової системи.
b) Використання хакерських програм для деблокування веб-фільтрів.
c) Зміна налаштувань операційної системи.

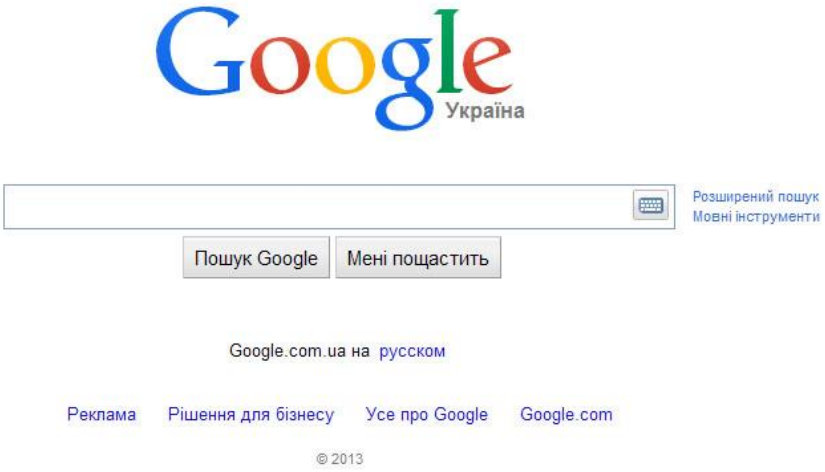
3) Налаштування безпечного пошуку в Google та Яндекс

http://www.yandex.ua



Зайшовши на сайт пошукової системи Яндекс у верхній правій частині екрану натисніть кнопку **Налаштування** і оберіть пункт **Інші налаштування**. Перейдіть у розділ **Налаштування результатів пошуку** та оберіть **Родинний пошук** у розділі Фільтрація сторінок.

https://www.google.com.ua



На пошуковій сторінці Google натисніть кнопку **Параметри** 

Налаштуйте **Фільтр Безпечного пошуку**

- **Безпечний пошук Google** вилучає з результатів пошуку веб-сторінки, які містять матеріали відвертого сексуального характеру.
- **Застосувати строгу фільтрацію** (Фільтрувати і відверті тексти, і відверті зображення)

Після виставлення параметрів потрібно зберегти налаштування пошуку.

Подібні налаштування пошукових систем працюватимуть для авторизованих користувачів у всіх браузерах, неавторизовані – будуть користуватися безпечним пошуком до очищення кеш-пам'яті браузера, в якому відбувалося налаштування.

Обхід захисту:

a) Відключення безпечного пошуку в системах Google та Yandex шляхом зміни відповідних параметрів пошуку.
b) Очищення кеш-пам'яті браузера, скидання налаштувань браузера на замовчувані.
c) Вихід з облікового запису пошукової системи.
d) Встановлення альтернативного браузера (або використання портабельної версії браузера).

Слід зауважити, що використання спеціального програмного забезпечення та налаштування операційної системи не дає можливості захистити дитину на 100% від шкідливого впливу глобальної мережі. Всі наведені міри захисту персонального комп'ютера та користувача Інтернету навіть в комплексі можуть лише частково вирішувати поставлене завдання.

Адже використання сучасних гаджетів – мобільних телефонів, смартфонів, планшетів для підключення та виходу в мережу Інтернет, миттєво усуває будь-які обмеження доступу до веб-сайтів з небезпечним для дитини контентом. Технічно реалізувати контроль і обмеження на таких пристроях на сьогодні практично неможливо.

Таким чином, використання ІКТ в освітньому процесі має відбуватися відповідно до законодавства української держави, морально-етичних норм. Використання на домашніх ПК та комп'ютерах навчальних закладів спеціального програмного забезпечення, налаштування операційних та мережевих систем в навчальних закладах є лише частковим вирішенням проблеми захисту дітей від шкідливого впливу глобальної мережі. Головним і обов'язковим елементом сучасної інформаційної освіти є забезпечення дітей знаннями про ризики й загрози ІКТ, формування в них свідомого й критичного мислення, виховання моральних і етичних рис.

Висновки

Отже, за допомогою технічних засобів можна зменшити ризики негативного впливу Інтернету на дитину. Але лише при доступі в Інтернет з комп'ютера, в той час як портативні пристрої, планшети і смартфони не дозволяють реалізувати такі налаштування. Крім того, жоден програмний продукт, навіть на комп'ютері, не забезпечить стовідсоткового захисту від шкідливої інформації та взаємодії з кібер-злочинцями. Тож технічний захист – це швидше додаткова міра.

Основним засобом захисту дитини в Інтернет-просторі є правильне інформаційне виховання, витоки якого починаються в сім'ї і підтримуються в навчальному закладі. Лише за таких умов психічне та фізичне здоров'я неповнолітніх користувачів глобальної мережі може перебувати у відносній безпеці.

Список використаних джерел

1. Бугайова Н.М. Віртуальні романтичні стосунки в Інтернеті, кіберсексуальна залежність. – Актуальні проблеми психології: Психологічна теорія і технологія. К., 2008, - Т.8, вип. 5
2. Бугайова Н.М. Інтернет-адикція як форма залежної поведінки.//Теорія та методика навчання математики, фізики, інформатики. – Кривий Ріг, 2006, Т.3, вип. VI, 408 с.
3. Кочарян А.Б., Гущина Н.І. Виховання культури користувача Інтернету. Безпека у всесвітній мережі. – К., 2011. – 100 с.
4. Литовченко І.В. Діти в Інтернеті: як навчити безпеці у віртуальному світі. – К., 2010, – 48 с.
5. Інтернет середовище як фактор психологічного розвитку комунікативного потенціалу особистості: Автореф. дис. канд. психол. наук: 19.00.07/ В.М. Фатурова, Ін-т психології імені Г.С. Костюка АПН України. – К., 2004.
6. Дайнека, Н. М., Кулик, Є. В. (2010) Кібербулінг як педагогічна проблема. Всеукраїнська науково-практична конфренція "Сучасні проблеми підготовки вчителя і його професійного удосконалення", Чернігівський національний педагогічний університет імені Т.Г. Шевченка.
7. https://uk.wikipedia.org/ – Україномовний розділ відкритої багатомовної мережевої енциклопедії Вікіпедія.
8. http://www.prointernet.in.ua/ – Про Інтернет.

Словник комп’ютерних термінів

(https://uk.wikipedia.org)

USB флеш-накопи́чувач (скор. UFD, сленгове — флешка) — носій інформації, що використовує флеш-пам'ять для збереження даних та підключається до комп'ютера чи іншого пристрою через USB-порт.

Антивірусна програма (антивірус) — програма для знаходження і лікування програм, що заражені комп'ютерним вірусом, а також для запобігання зараження файлу вірусом.

Брандмауер — програма чи пристрій, що здійснює захист комп'ютерних мереж.

Бра́узер (англ. browser) — програмне забезпечення для комп'ютера або іншого електронного пристрою, що дає можливість користувачеві взаємодіяти з текстом, малюнками або іншою інформацією на гіпертекстовій веб-сторінці.

Вішинг (vishing - voice phishing) названий так за аналогією з фішингом - поширеним мережевим шахрайством. Подібність назв підкреслює той факт, що принципової різниці між вішинг і фішингом немає. Основна відмінність вішинг в тому, що так чи інакше задіюється телефон.

Всесві́тня мережа (англ. World Wide Web, скорочено: WWW; також: всемережжя, веб або тене́та) — найбільше всесвітнє багатомовне сховище інформації в електронному вигляді: десятки мільйонів пов'язаних між собою документів, що розташовані на комп'ютерах, розміщених на всій земній кулі.

Гіперпосила́ння — це активний (виділеним кольором) текст, зображення чи кнопка на веб-сторінці, натиснення на яку (активізація гіперпосилання) викликає перехід на іншу сторінку чи іншу частину поточної сторінки.

Грифери – інтернет-шахраї, які заважають учасникам он-лайн ігор спокійно грати. Вони пошкоджують віртуальних персонажів, викрадають їх, блокують функції гри тощо.

До́мен (англ. Domain) — частина простору ієрархічних імен мережі Інтернет, що обслуговується групою серверів доменних імен (DNS-серверів) та централізовано адмініструється.

Електро́нна по́шта (англ. e-mail, або email, скорочення від electronic mail) — популярний сервіс в інтернеті, що робить можливим обмін даними будь-якого змісту (текстові документи, аудіо-, відео-файли, архіви, програми).

Інтерне́т (від англ. Internet) — всесвітня система взаємосполучених комп'ютерних мереж, що базуються на комплекті Інтернет-протоколів.

Інтернет-фільтр (контент-фільтр) — програма для обмеження доступу до інтернет-ресурсів.

Кібербулінг – переслідування особи з використанням сучасних електронних технологій та інших засобів електронної техніки.

Кібергрумінг – входження в довіру дитини з метою використання її в сексуальних цілях.

Комп'ютерний вірус (англ. computer virus) — комп'ютерна програма, яка має здатність до прихованого саморозмноження. Одночасно зі створенням власних копій віруси можуть завдавати шкоди: знищувати, пошкоджувати, викрадати дані, знижувати або й зовсім унеможливлювати подальшу працездатність операційної системи комп'ютера.

Контент — інформаційне наповнення сайту.

Нік, Нікнейм (від англ. nick, nickname — прізвисько, анонім) — особисте, переважно, вигадане, ім'я, яким називають себе користувачі інтернету в різноманітних чатах, форумах, месенджерах, а також у Вікіпедії, на сайтах та вікі-сайтах.

Обліковий запис у комп'ютерній системі — сукупність наданої інформації про користувача, засобів та прав користувача відносно багатокористувацької системи.

Онлайн (англ. online, від англ. on line — «на лінії», «на зв'язку», «у мережі», «в ефірі») — «такий, що знаходиться у стані підключення».

Пошукова́ систе́ма — онлайн-служба (програмно-апаратний комплекс з веб-інтерфейсом), що надає можливість пошуку інформації в Інтернеті.

Про́ксі-се́рвер (від англ. proxy — «представник, уповноважений») — сервер (комп'ютерна система або програма) в комп'ютерних мережах, що дозволяє клієнтам виконувати непрямі запити до мережевих сервісів.

Сайт або веб-сайт (від англ. website, місце, майданчик в інтернеті) — сукупність веб-сторінок, доступних у мережі Інтернет, які об'єднані як за змістом, так і за навігацією. Фізично сайт може розміщуватися як на одному, так і на кількох серверах.

Се́рвер — це комп'ютер у локальній чи глобальній мережі, який надає користувачам свої обчислювальні і дискові ресурси, а також доступ до встановлених сервісів.

Смайл, сма́йлик (від англ. smile — усмішка), також емотико́н, емогра́ма (англ. emoticon) — схематичне зображення людського обличчя, що використовується для передачі емоцій.

Спам (англ. spam) — масова розсилка кореспонденції рекламного чи іншого характеру людям, які не висловили бажання її одержувати.

Тро́лінг (від англ. trolling) — розміщення в Інтернеті (на форумах, у групах новин Usenet, у вікі-проектах та ін.) провокаційних повідомлень з метою викликати флейм, конфлікти між учасниками, образи, війну редагувань, марнослів'я тощо.

Фі́шинг (англ. phishing) — вид шахрайства, метою якого є виманювання у довірливих або неуважних користувачів мережі персональних даних клієнтів онлайнових аукціонів, сервісів з переказування або обміну валюти, інтернет-магазинів.

Фармінг – перенаправлення жертви із завантаженого веб-узла на клон сайта, який хотів відвідати користувач. Далі відбувається зараження вірусами комп’ютера.

Фейк – фальсифікована інформація.

Хо́стинг (англ. hosting) — послуга, що надає дисковий простір для розміщення фізичної інформації на сервері, що постійно перебуває в мережі (наприклад Internet).

Чат (англ. chat — «балачка») — мережевий засіб для швидкого обміну текстовими повідомленнями між користувачами Інтернету у режимі реального часу.