ЄДИНА СИСТЕМА ОБМЕЖЕННЯ ДОСТУПУ ДО НЕЦІЛЬОВИХ РЕСУРСІВ МЕРЕЖІ ІНТЕРНЕТ В ОСВІТНІХ ЗАКЛАДАХ УКРАЇНИ

Воробієнко П.П., Каптур В.А., Коляденко В.А., Самодід В.О.

Анотація. Проведено аналіз світового досвіду обмеження доступу до нецільових ресурсів мережі Інтернет. Розглянуто найбільш розповсюджені механізми обмеження доступу до нецільових інформаційних ресурсів мережі Інтернет. Запропоновано концепцію створення єдиної системи обмеження доступу, яка передбачає централізоване збереження бази даних нецільових ресурсів. Розглянуто аспекти практичної реалізації пропонованої системи, а також основні напрями її розвитку.

Ключові слова: обмеження доступу, нецільові ресурси, Інтернет, proxy-сервер.

Зростаючі темпи інформатизації загальноосвітніх середніх шкіл та навчальних закладів всіх рівнів, які обумовлені виконанням низки державних цільових програм [1–4] щодо оснащення освітніх закладів комп'ютерною технікою та підімкненням до мережі Інтернет, поставили перед Україною важливе завдання — забезпечення ефективного використання цієї техніки та орендованих ресурсів. Відомо, що мережа Інтернет (у більшій своїй частині) є практично нерегульованою та наповнюється самою різноманітною інформацією: від наукових статей до нецільових ресурсів. Слід зазначити, що до ресурсів, які в межах цієї статті позначаються як «нецільові», у першу чергу, відносяться такі, що прямо ведуть пропаганду насилля, містять нецензурну лексику або/та носять відкритий порнографічний характер. За інформацією європейської комісії, більш ніж 44% дітей, які користуються Інтернетом, стикаються з порнографічними та іншими небажаними матеріалами. За таких умов підтримка належного рівня культури та моральності в навчальних закладах стає практично непосильним завданням.

Вирішенням цієї проблеми може стати встановлення контролю за цільовим використанням каналів доступу до мережі Інтернет у вигляді обмеження доступу до нецільових (у тому числі порнографічних та таких, що ведуть пропаганду насилля) інформаційних ресурсів. У різних країнах світу мають різні погляди на регулювання ситуацій з питань моральності, порнографічних ресурсів, таємниці особистого життя та даних. Наприклад, п'ять найбільших Інтернет-провайдерів Німеччини підписали угоду про блокування доступу до дитячої порнографії. У тому ж напрямку працюють державні програми у Великобританії та Канаді. У цих країнах працює проект під назвою Cleanfeed [5] .

З 2004 року у Франції вживаються активні адміністративні заходи, які забезпечують захищений доступ у навчальних закладах [6]. Уряд країни централізовано запровадив контентні фільтри, які забороняють доступ до сайтів фашистського напрямку, а також до порноресурсів.

У липні 2007 року в Таїланді набув чинності закон, який дозволяє поліції вилучати особисті комп'ютери у приватних осіб, котрі підозрюються у розповсюдженні порнографічних матеріалів [7]. Тією чи іншою мірою, країни Персидської затоки, такі як Іран, Судан та Туніс, блокують контент, котрий має відношення до порнографії, знайомств та непристойного одягу [8].

У 2006 у Венесуелі Національна Асамблея прийняла закон із захисту дітей від нецензурного змісту в мережі, який вимагає від провайдерів вилучати нецензурний контент зі своїх серверів та надавати фільтруючі програми для користувачів, з метою сприяння саморегулювання [9]. У Перу обмежуючі програми обов'язкові для всіх комп'ютерів в організаціях, де вони можуть бути використані дітьми для доступу в мережу Інтернет [10].

Отже, актуальність питання захисту дітей у мережі Інтернет від негативної інформації підтверджується зацікавленістю світової спільноти та прийняттям відповідних законодавчих актів.

Метою статті є розробка концепції єдиної системи обмеження доступу до нецільових ресурсів мережі Інтернет в освітніх закладах України.

Слід зазначити, що всі можливі підходи до обмеження доступу можна умовно поділити на два класи:

— «усе, що прямо не дозволено, те заборонено». Такий підхід більш притаманний організаціям, які мають чітко визначене коло інтересів та мають перелік цільових ресурсів;

— «усе, що прямо не заборонено, те дозволено». Більш характерний для організацій та закладів, які займаються науковою діяльністю та освітою.

Нині існує декілька найбільш розповсюджених механізмів обмеження доступу до нецільових ресурсів мережі Інтернет із комп'ютерних мереж окремих організацій. Серед таких механізмів слід зазначити:

а) блокування доступу до нецільових ресурсів за IP-адресою (окремого вузла або підмережі в цілому) із використанням міжмережевих екранів на маршрутизаторах доступу або робочих станціях [11–12];

б) використання функцій обмеження доступу вбудованих до веб-браузерів [13];

в) застосування механізмів фільтрації нецільових ресурсів на proxy-серверах, що розташовуються в межах мережі організації [14];

г) фільтрація нецільових ресурсів на DNS-серверах, які належать провайдеру, організації, або безпосередньо на робочих станціях [15].

Порівняльний аналіз (із зазначенням основних переваг та недоліків) розглянутих вище методів наведено в табл. 1.

Усі з перерахованих в табл. 1 методів тією чи іншою мірою можливо використати в централізованій чи децентралізованій схемі.

Централізована схема передбачає обробку навантаження на центральному вузлі, котрий надає свої сервіси для користувачів. При цьому обробка може проводитися будь-яким із вищезазначених способів, окрім фільтрування за допомогою функцій вбудованих у веб-браузер. Незважаючи на те, що така схема дозволяє отримати повний контроль та швидко реагувати на появу нових нецільових ресурсів, вона має низку досить суттєвих недоліків:

— обладнання, яке буде займатися обробкою, повинно мати відповідну потужність, щоб не вносити велику затримку та не створювати незручності користувачам;

— центральний вузол повинен мати велику пропускну здатність каналів зв'язку;

— у разі виходу з ладу центрального вузла система перестає функціонувати.

Децентралізована схема передбачає фільтрацію навантаження безпосередньо на місцях. Це можуть буди як кінцеві робочі станції, так і вузлове обла-

Таблиця 1

Назва методу	Переваги	Недоліки
Блокування за IP-адресою	– надійний спосіб, котрий повністю обмежує доступ до вузлів, котрі підходять під критерії фільтрації; – доступність обладнання та програмного забезпечення, котрі реалізують зазначений механізм фільтрації; – можливість реалізації як на вузлових маршрутизаторах, так і в кінцевого користувача	– у разі великої кількості записів у списках фільтрації, зростає навантаження на обладнання, котре реалізує фільтрацію; – оптимізація та агрегація не надають великого виграшу і з'являється можливість помилково обмежити доступ до ресурсів, котрі не підпадають під жоден із критеріїв, за якими проводиться оцінювання. Також сама задача оптимізації та агрегації не є тривіальною та за великої кількості чинників та критеріїв може буди дуже складною; – мала інформативність та відсутність діалогу з користувачем, котрий повідомляє користувачу, що доступ блоковано та причину, чому саме
Блокування за допомогою браузера	– не потребує високого рівня кваліфікації під час конфігурування; – доцільне використання за невеликого обсягу робочих комп'ютерів та невеликій базі списків обмеження	– складність адміністрування та підтримки списків заборонених ресурсів у разі зростання: кількості робочих вузлів (у даному випадку під вузлом розуміється робоча станція користувача); кількості записів у списках заборонених ресурсів; – обмеження працює тільки для певного браузера, у якому сконфігуроване обмеження; – складність збору та обробки статистичної інформації
Застосування proxy-серверів	– легкість масштабування. Можливість ієрархічної схеми розміщення proxy-серверів дозволяє легко нарощувати нові підключення; – у разі використання розподіленої мережі proxy-серверів, підвищується загальна відмовостійкість системи; – наявність адаптивного підходу під час впровадження та швидкого реагування на появу нових нецільових ресурсів; – суттєве зменшення загального http-трафіку, за рахунок кешування інформації	– необхідність обмеження навантаження відмінного від HTTP; – необхідність застосування додаткових методів оптимізації за великої кількості користувачів у межах однієї мережі
Фільтрація на DNS	– немає необхідності встановлення додаткового програмного забезпечення на кінцеві комп'ютери, у разі використання централізованого серверу DNS; – централізоване керування загальними списками обмеження, що полегшує адміністрування системи в цілому; – легкість масштабування	– необхідно конфігурувати кожну робочу станцію окремо; – вноситься додаткова затримка під час обробки запиту; – можливість обходу системи обмеження на клієнтських комп'ютерах, конфігуруванням іншого DNS-серверу або внесенням запису до hosts-файлу

днання. До центрального вузла передається лише статистична інформація, у простішому випадку — лог-файл зі списком адрес відвіданих ресурсів. У центральному вузлі проводиться обробка статистичної інформації та формування актуальних списків заборонених ресурсів, після чого всі вузли системи оновлюють свої локальні списки зі списками центрального вузла. Така схема дозволяє зменшити вимоги до центрального вузла та підвищити відмовостійкість, оскільки кожен вузол функціонує автономно та лише оновлює з центрального вузла списки заборонених ресурсів. Певним недоліком такого підходу є те, що оновлення списків заборонених ресурсів проходить повільніше, ніж у централізованій системі, це зумовлено періодом формування статистичної інформації.

Виходячи з порівняльного аналізу, наведеного в табл. 1, а також враховуючи зазначені вище переваги децентралізованої схеми, в основу пропонованої в цій статті системи обмеження доступу до нецільових ресурсів мережі Інтернет пропонується покласти принцип встановлення в кожному навчальному закладі України власного proxy-серверу, який має базу даних заборонених ресурсів.

Базові принципи фільтрації ресурсів із використанням проксі-сервера зображено на рис. 1.

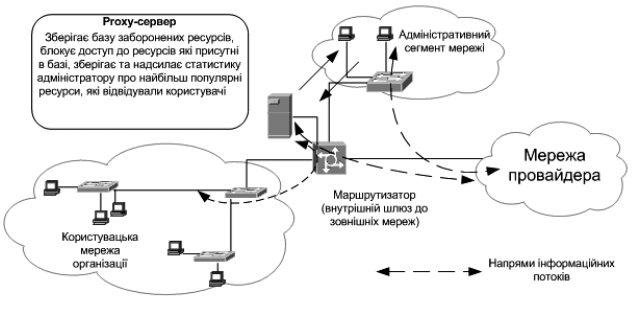

Рис. 1

Згідно зображеного принципу користувачі комп'ютерної мережі певної організації одержують доступ до мережі Інтернет виключно через proxy-сервер. Безпосередній доступ до мережі для користувачів мережі повністю заблоковано на маршрутизаторі.

За кожної спроби одержання доступу до того чи іншого ресурсу proxy-сервер перевіряє, чи не внесено його до переліку нецільових. У разі, якщо такий ресурс позначено в базі нецільових — доступ до нього блокується, а користувачу видається на екран відповідне повідомлення. Приклад такого повідомлення наведено на рис. 2.

У разі, якщо запитаний ресурс відсутній у базі заборонених ресурсів, то доступ до нього надається, однак запис про відвідування цього ресурсу фіксується в спеціальному службовому журналі. Один раз на день (або в інший термін) proxy-сервер формує перелік найбільш відвідуваних ресурсів та надсилає його оператору з обмеження доступу. Оператор (адміністратор) перевіряє надісланий перелік ресурсів

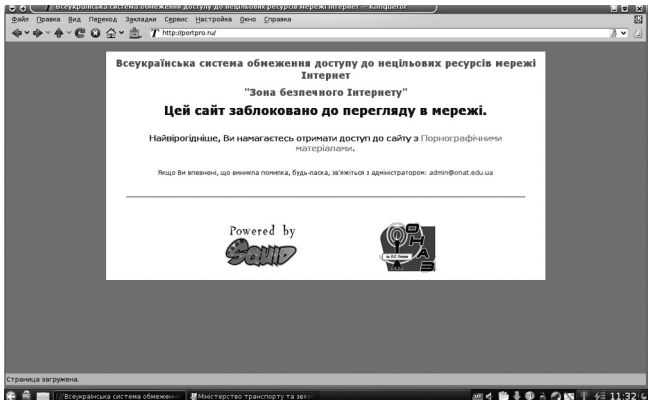

Рис. 2

та визначає їх характер (нецільові або корисні). У разі, якщо ресурс має нецільовий характер здійснюється його класифікація (порнографічний ресурс, ігровий ресурс, ресурс, який використовується для обходу заборони, тощо) та формується доповнення до бази даних.

Загальні принципи діяльності пропонованої системи зображені на рис. 3. В основу системи покладено принцип встановлення в кожному навчальному закладі власного proxy-серверу, який має базу даних заборонених ресурсів. З метою її початкового наповнення та постійного оновлення пропонується організувати централізовану обробку службових журналів зазначених серверів на базі інформаційного центру з подальшим періодичним (наприклад, щотижня) формуванням оновленої редакції бази даних заборонених ресурсів та її розсиланням (в автоматичному режимі) по всіх запроваджених proxy-серверах.

З метою дослідної експлуатації пропонована система була розгорнута на базі декількох шкіл Одеської області та в межах навчальних корпусів та гуртожитків Одеської національної академії зв'язку ім. О.С. Попова. Станом на листопад 2009 року існуюча база інформаційних ресурсів, які використовуються для блокування, налічує близько 250 тисяч записів у сімох категоріях.

Використане під час реалізації дослідного сегмента програмне забезпечення розповсюджується вільно, тому не потребує додаткових коштів на ліцензування. Такий вибір дозволяє використовувати адаптивний підхід до кожного конкретного випадку та впроваджувати систему мінімальними змінами в існуючій інфраструктурі організації.

Слід також зазначити, що використання пропонованого підходу дозволяє постійно поповнювати перелік заблокованих ресурсів пропорційно тому, як нові ресурси з'являються в мережі Інтернет.

Вартість реалізації такої системи в межах однієї організації (наприклад, середньої школи, вищого навчального закладу або державної установи) буде залежати від конкретної реалізації мережі (наявність або відсутність виділеної апаратної платформи для організації proxy-серверу, спосіб організації доступу до мережі Інтернет тощо). Однак, зважаючи на мо-

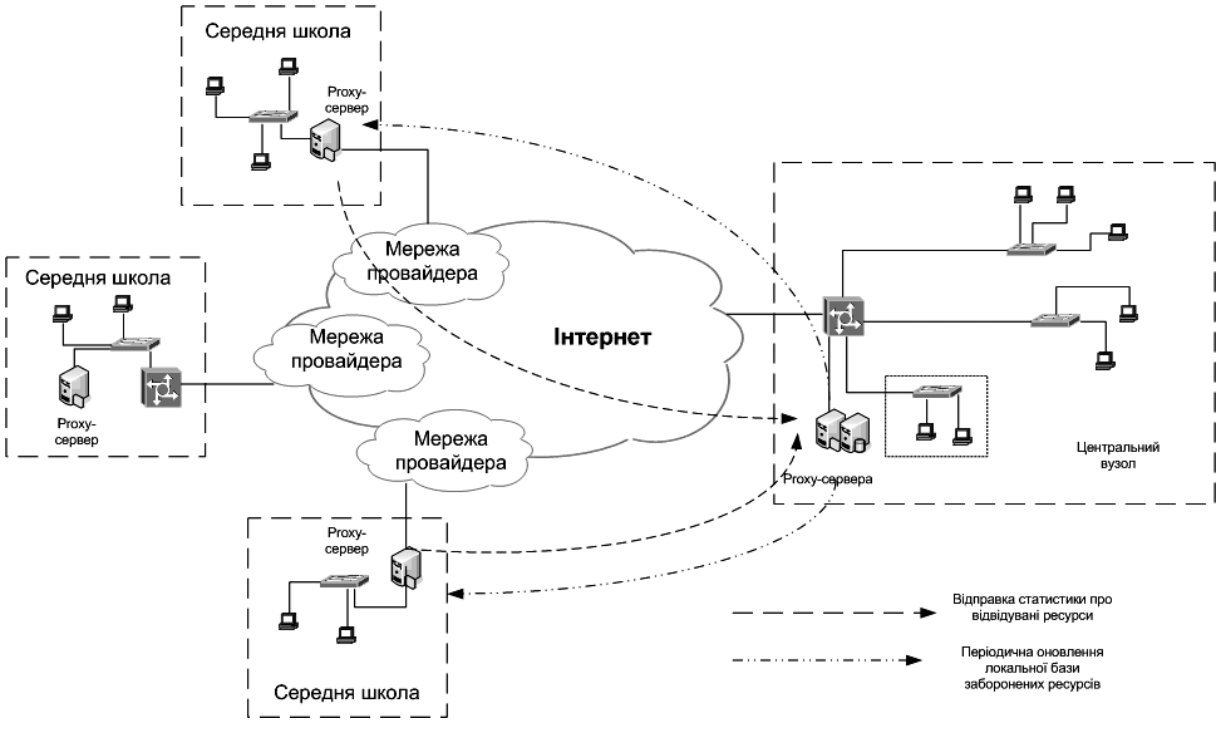

Рис. 3

жливе використання в цьому рішенні безкоштовного програмного забезпечення, вартість запровадження системи обмеження доступу до нецільових ресурсів мережі Інтернет залежить переважно від вартості апаратних платформ (слід зазначити, що подекуди для розміщення програмного забезпечення proxy-серверу можуть використовуватися вже існуючі в організації робочі станції), а також від вартості робіт на його розгортання.

Слід зазначити, що першочерговим об'єктом уваги для запровадження такої системи мають стати загальноосвітні середні школи, які вже сьогодні, маючи у своєму розпорядженні канали доступу до мережі Інтернет практично не обмежені у сприйманні інформаційних ресурсів, розміщених у цій мережі.

Орієнтовна вартість впровадження системи для всіх загальноосвітніх середніх шкіл у межах України складає близько 30 млн. грн. та складається з трьох основних складових: вартості обладнання (82%), оплати відряджень (13%) та витрат на оплату праці (5%).

Подальший розвиток пропонованої системи може здійснюватися як шляхом підімкнення до неї нових організацій (у тому числі державних органів влади та приватних компаній тощо), так і переведенням її в іншу площину — надання послуг фізичним особам шляхом обмеження доступу до нецільових ресурсів для їх домашніх станцій (через підключення провайдерів до пропонованої системи).

Висновки та результати

1. Запропонований у роботі підхід до захисту дітей у мережі Інтернет має низку суттєвих переваг порівняно з іншими аналогічними підходами.

2. Порівняно незначна вартість реалізації системи в межах країни за величезного соціального ефекту дозволяє сподіватися на його підтримку як державними інституціями, так і благодійними організаціями.

3. Впровадження системи обмеження доступу до нецільових ресурсів дозволяє значно підвищити рівень моральності населення України.

4. Комп'ютерна техніка, використана для запровадження системи, може також бути застосована в середніх школах для забезпечення навчального процесу.

5. Зменшення вартості впровадження та збільшення ефективності застосування пропонованого рішення можливе за рахунок проведення низки додаткових досліджень: розробки методик визначення найбільш ефективного способу підімкнення нових об'єктів до системи, оптимізація існуючого програмного забезпечення; аналіз використання ієрархічних структур proxy-серверів; розробка та узаконення вимог до політики безпеки шкільних мереж тощо.

* * *

Воробиенко П.П., Каптур В.А., Коляденко В.А., Самодед В.О. Единая система ограничения доступа к нецелевым ресурсам сети Интернет в учебных заведениях Украины

Аннотация. Проведён анализ мирового опыта ограничения доступа к нецелевым ресурсам сети Интернет. Рассмотрены наиболее распространенные механизмы ограничения доступа к нецелевым информационным ресурсам сети Интернет. Предложена концепция создания единой системы ограничения доступа, предполагающей централизованное хранение базы данных нецелевых ресурсов. Рассмотрены аспекты практической реализации предложенной системы, а также основные направления её развития.

Ключевые слова. Ограничение доступа, нецелевые ресурсы, Интернет, proxy-сервер.

Література

1. Державна програма роботи з обдарованими молоддю на 2007–2010 роки (Постанова Кабінету Міністрів України від 8 серпня 2007 р. №1016).
2. Указ Президента України №928/2000 від 31 липня 2000 року «Про заходи щодо розвитку національної складової глобальної інформаційної мережі Internet і забезпеченню широкого доступу до цієї мережі в Україні».
3. Національна доктрина розвитку освіти (Затверджено Указом Президента України від 17.04.2002 р. №347/2002).
4. Указ Президента України №1013 від 4 липня 2005 року «Про невідкладні заходи щодо забезпечення функціонування та розвитку освіти в Україні».
5. Project Cleanfeed, [Електроний ресурс]. — Режим доступу: http://en.wikipedia.org/wiki/Cleanfeed_(content_blocking_system).
6. Usage de l'internet dans le cadre pйdagogique et protection des mineurs (CIRCULAIRE N°2004-035 DU 18-2-2004). [Електронний ресурс]. — Режим доступу: http://www.education.gouv.fr/bo/2004/9/MENT0400337C.htm.
7. В Таиланде новый закон позволяет полиции изымать частные компьютеры / Федор Карымов, [Електронний ресурс]. — Режим доступу: http://www.zakon.kz/90418-v-tailande-novyjj-zakon-pozvoljaet.html.
8. Study Finds 25 Countries Block Web Sites, [Електронний ресурс]. — Режим доступу: http://www.smh.com.au/news/breaking-news/study-finds-25-countries-block-web-sites/2007/05/18/1178995390626.html.
9. Law no. 38.529, Asamblea Nacional de la Republica Bolivariana de Venezeula, «Ley de Protecci?n de Ni?os, Ni?as y Adolescentes en salas de uso de Internet, V?deo Juegos y otros Multimedia», November 5, 2006.
10. LEY QUE ESTABLECE LA OBLIGACIYN DE FILTROS ANTIPORNOGRЂFICOS EN INSTITUCIONES EDUCATIVAS Y BIBLIOTECAS QUE BRINDEN ACCESO A INTERNET. [Електронний ресурс]. — Режим доступу: http://www2.congreso.gob.pe/Sicr/RelatAgenda/proapro.nsf/ProyectosAprobadosPortal/E72D2E5A68F3267E0525715400031C02/$FILE/12756Filtrosantipornograficos.pdf.
11. Oskar Andreasson. Руководство по iptables. [Електронний ресурс]. — Режим доступу: http://www.opennet.ru/docs/RUS/iptables/.
12. Microsoft . How to Configure Windows Firewall in a Small Business Environment Using Group Policy. [Електронний ресурс]. — Режим доступу: http://technet.microsoft.com/en-us/library/cc875816.aspx#EBJAC.
13. ICRA filtering using Microsoft Internet Explorer. [Електронний ресурс]. — Режим доступу: http://www.icra.org/support/contentadvisor/setupv03.
14. Squid-cache wiki. Blocking Content Based on MIME Types. [Електронний ресурс]. — Режим доступу: http://wiki.squid-cache.org/ConfigExamples/BlockingMimeTypes?highlight=(ConfigExamples/Chat)|(ConfigExamples/Authenticate)|(ConfigExamples/Streams)|(ConfigExamples/Intercept)|(ConfigExamples/Strange)|(ConfigExamples/Reverse).
15. Project OpenDNS. [Електронний ресурс]. — Режим доступу: http://www.opendns.com/solutions/overview/.

* * *

Відгуки можна надсилати на адресу: **vadim.kaptur@onat.edu.ua**.

Від редакції. Враховуючи важливість зазначеної проблеми, після виходу у світ журналу стаття буде передана у Комітет Верховної ради з питань науки і освіти.

* * *

ПЕРШІ КРОКИ ДО ІНТЕРНЕТУ

Бондаренко С.М.

З кожним роком в Україні зростає аудиторія користувачів Інтернету. До Інтернету приєднуються й діти, й дорослі. Про Інтернет написано багато статтей, видано величезну кількість книжок. Але більшість з них розрахована на досвідченних користувачів. Для дорослих і дітей завжди виникає питання: з чого почати? Сподіваємося, що ця стаття допоможе як дітям, так і їхнім батькам зробити перші впевнені кроки до оволодіння професійними навичками роботи в Інтернеті.

Якщо два чи більше комп'ютерів об'єднати між собою, то отримаємо **комп'ютерну мережу**. Для чого це робити? Щоб передавати інформацію на близьку чи далеку відстань, спілкуватися за допомогою комп'ютера, користуватися спільною технікою (наприклад, якщо користувачів багато, а принтер чи сканер один) тощо. Мережі також об'єднують між собою.

Чи відомо тобі, що…
*… **мова HTML**, за допомогою якої створюють сайти, дозволяє форматувати текст, створювати гіперпосилання, додавати картинки чи анімаційні елементи, звукозапис чи таке інше. Ці файли обробляються броузером та дозволяють тобі бачити сайт у всій його красі на моніторі…*

Отже, **Інтернет** — це велика кількість комп'ютерних мереж по всьому світу, які об'єднані між собою. Уявіть собі, за допомогою Інтернету люди всього світу, незважаючи на кордони, не відходячи від свого комп'ютера, можуть шукати потрібну інформацію, обмінюватись книгами (звісно, електронними!), писати листи, спілкуватися, купувати потрібні речі та багато іншого.

Об'єднання різних комп'ютерних мереж стало можливо за допомогою використання протоколу **TCP/IP** (читається «ті-сі-пі / ай-пі»). **Протокол** — це «мова», яку використовує комп'ютер для обміну інформацією під час роботи в мережі. Щоб різні комп'ютери могли працювати разом, вони повинні «розмовляти» однією «мовою», тобто використовувати один протокол.

Спеціальна програма — **браузер** — допомагає представити інформацію так, щоб її можна було прочитати. Найрозповсюдженіший браузер, який, можливо, встановлений на комп'ютері — Internet Explorer, позначений ось такою позначкою  .

Уся інформація в Інтернеті розміщується на так званих сайтах. **Веб-сайт** (рис. 1) чи просто **сайт** (*англ.* website, від web — павутина і site — місце) — це одна чи декілька веб-сторінок, які можна прочитати в Інтернеті. Сторінки мають загальну адресу (наприклад, www.yandex.ru), загальну тему, оформлення