БЕЗПЕКА СЕРФІНГУ В ІНТЕРНЕТІ

Хачіров Т.С.

У рамках реалізації Державної національної програми «Освіта» («Україна XXI століття»), спрямованої на виведення освіти в Україні на рівень освіти розвинутих країн світу, Закону України «Про Національну програму інформатизації», Державної цільової програми «Сто відсотків» проводяться широкомасштабні заходи щодо запровадження інформаційно-комунікаційних технологій у навчальний процес загальноосвітньої школи, забезпечення навчальних закладів швидкісним доступом до Інтернету. Як наголошує президент Національної академії педагогічних наук України В.Г. Кремень, це означає оновлення школи, перехід «до відкритої навчальної архітектури із забезпеченням дійсно індивідуалізованого, особистісно-орієнтованого навчання, заснованого на застосуванні інформаційних технологій» [1].

Можливість використовувати Інтернет безпосередньо на уроці породжує низку завдань, що стосуються підготовки педагогічних кадрів до ефективної професійної діяльності в умовах інтернетизованої школи, проте особлива проблема полягає в тому, щоб процес використання Інтернету був захищеним від небезпек і ризиків, з якими пов'язана діяльність у мережі. У Концепції державної цільової програми «Сто відсотків» одним з важливих завдань визнано «забезпечення інформаційної безпеки та централізованого фільтрування несумісного з навчальним процесом контенту» [2]. Зазначена проблема має знайти своє відображення у системі підготовки вчителя інформатики, професійні обов'язки якого включають як навчання школярів основ Інтернет-технологій та їх застосування, так і організацію належного функціонування кабінету інформатики в умовах наявності доступу до мережі Інтернет, включаючи дотримання низки вимог щодо використання ліцензійного програмного забезпечення, захисту персональних даних користувачів, недопущення контакту учнів з контентом, який може негативно впливати на їхню свідомість, тощо.

Питання безпеки в процесі використання Інтернету відносяться до широко обговорюваних у педагогічній літературі [3, 4, 5]. З огляду на те, що в Україні широкомасштабні процеси інтернетизації загальноосвітніх навчальних закладів розпочалися тільки в останні роки й припали на період інтенсивного розвитку самої мережі Інтернет, доречно скористатися досвідом вирішення розглядуваних питань в освітянській практиці зарубіжжя, водночас ураховуючи і перспективні напрями трансформації глобальної мережі. На підставі аналізу попередніх досліджень автори роботи [6] пропонують комплексний підхід до розв'язання проблеми он-лайн безпеки, основу якого складає поєднання заходів організаційного і виховного характеру з програмно-апаратними способами регулювання доступу до ресурсів мережі, здійснення контролю за діями користувача і фільтрації контенту. Не знижуючи ролі організаційних заходів і значимості різнопланової виховної роботи зі школярами в напрямі формування у них умінь безпечної роботи в Інтернеті, слід підкреслити, що в умовах шкільного навчального процесу визначальну роль у системі забезпечення належних умов роботи учнів в Інтернеті мають відігравати програмні засоби фільтрації контенту.

Метою даної статті є порівняльний аналіз доступних на цей час засобів фільтрації web-контенту в комп'ютерному класі.

Розглянемо технічні аспекти серверної фільтрації. Якщо ми маємо виділений сервер з доступом до мережі Інтернет, і цей доступ також надається іншим комп'ютерам через локальну мережу, то можна говорити про можливість фільтрації контенту на шлюзі. Відомими програмами для організації серверної контент-фільтрації є: МКФ, Usergate, Kerio; ISA Server, Safesquid — для Windows; Dansguardian, Mindwebfilter — для Linux. Великим недоліком рішень під ОС Windows є те, що майже всі вони платні, а якщо й безкоштовні, як МКФ, то вимагають інсталювання платного продукту. Перелічені програми для Linux є безкоштовними, але вони більш складні в налаштуванні.

Зупинимося на принципах клієнтської фільтрації. На кожному комп'ютері, де потрібна контент-фільтрація, встановлюється й налаштовується програма, яка це здійснює. Прикладами таких програм для Windows є:

Інтернет цензор (http://www.icensor.ru/);

ПКФ (http://skf.edu.ru/);

Netpolice (http://www.netpolice.ru/);

Kindergate (http://usergate.ru/products/kindergate_parental_control/).

Для Linux — Netpolice ALT Linux та ін. Однак зазначені програмні продукти є окремими додатками й вимагають окремого налаштування на кожному клієнтському комп'ютері, що не є зручним в умовах шкільного кабінету інформатики.

Однією з поширених практик блокування доступу до окремих сайтів є використання системи DNS та/або файлу hosts (який є присутнім у будь-якій операційній системі). Наприклад, створивши запис у файлі hosts, учитель може повністю блокувати сайт або перенаправити запит на інший сервер. Недоліками такого блокування є те, що, по-перше, потрібно внести зміни на всі комп'ютери, по-друге, блокується доступ до всього сайту, а не тільки до небажаної його частини або окремих сторінок.

Розглянемо досить простий безкоштовний спосіб контент-фільтрації, який у той же час є і досить ефе-

Рис. 1

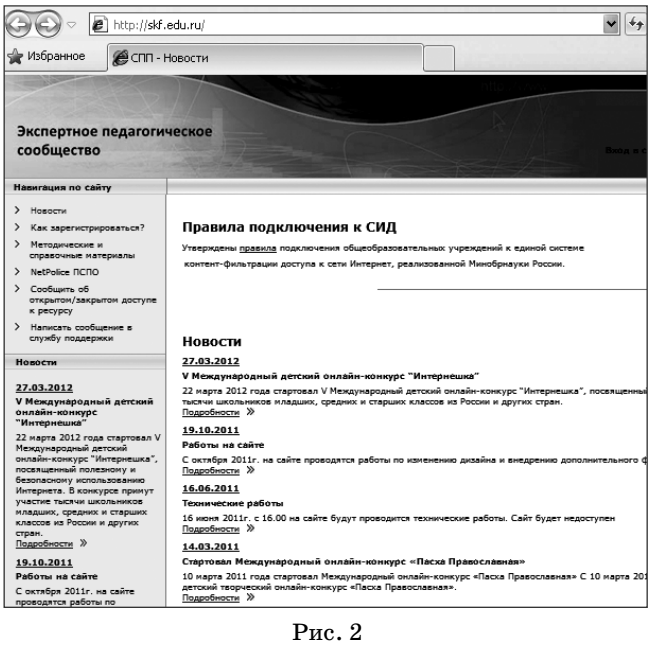

Рис. 2

активним. Його можна використовувати разом з кожним з інших способів як доповнення. Для його впровадження необхідне таке програмне забезпечення:

- будь-який з дистрибутивів ОС Windows або Linux;
- браузер Mozilla Firefox або браузери на його основі, що підтримують плагіни й розширення Firefox;
- підключення до Інтернету.

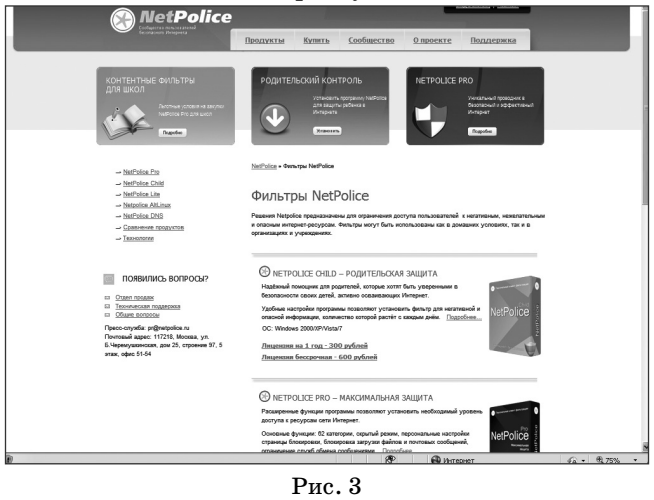

Рис. 3

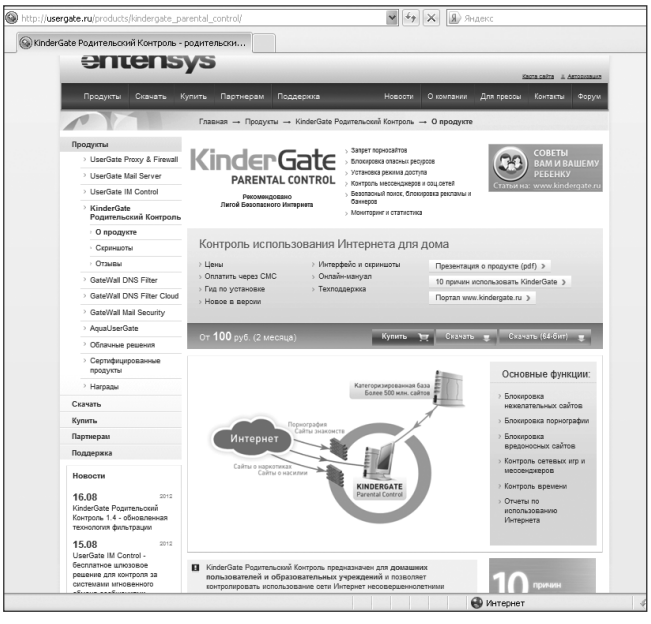

Рис. 4

У браузера Mozilla Firefox є безліч додаткових модулів. На їх основі і може бути здійснена контент-фільтрація. Розглянемо їх.

1. **WOT (Web of Trust)** — це безкоштовна надбудова до браузера, яка попереджає Інтернет-користувача під час пошуку інформації або здійснення покупок про потенційно небезпечні веб-сторінки. WOT є сумісним з такими браузерами як Internet Explorer, Mozilla Firefox, Opera (в 11 версії за допомогою розширення), Google Chrome. У модулі є функція батьківського контролю, яка також спрямована на лімітування використання сервісів мережі. За допомогою цього модуля можна якісно виконувати контент-фільтрацію.

2. **Adblock Plus** — розширення для браузерів й іншого ПЗ на основі Gecko: Mozilla Firefox (включаючи «мобільний»), Mozilla Thunderbird, Mozilla Suite, Seamonkey, Songbird і Mozilla Prism, що дозволяє блокувати завантаження й показ різних елементів сторінки: надмірно настирливих або неприємних рекламних банерів, спливаючих вікон й інших об'єктів, що заважають використанню сайту.

3. **Public Fox** потрібний для того, щоб діти не змогли відключити доповнення, відповідальні за контент-фільтрацію. За їх допомогою можна встановити пароль для налаштувань.

Фільтрацію пошукової видачі можна налаштувати засобами самого пошукового механізму, і в такий спосіб залишати для пошуку тільки безпечний Гугл-Пошук або сімейний пошук Яндексу. Водночас немає необхідності виконувати налаштування зазначених вище модулів на кожному комп'ютері. Досить скопіювати профіль Mozilla Firefox (профіль розташований у папці %APPDATA%\Mozilla\Firefox\Profiles\) і замінити цей профіль на іншому комп'ютері. Усі налаштування й модулі перенесуться на інший комп'ютер.

Щоб фільтр був ефективним, потрібно заборонити використання інших браузерів. В ОС Linux це вирішується легко — якщо браузер не один, за допомогою па-

кетного менеджера слід вилучити інші. В ОС Windows це вже складніше. Насамперед потрібно зробити теж саме — вилучити встановлені сторонні браузери. Залишається тільки Internet Explorer (далі IE) браузер за замовчуванням, який видаляти небажано. Тому необхідно зробити Firefox браузером за замовчуванням і вилучити всі ярлики IE з пуску й робочого стола, ярлики швидкого запуску. У більшості випадків цього буде досить. Заборонити ж запуск IE можливо стандартними засобами ОС, наприклад, груповими політиками або через реєстр операційної системи.

Розглянемо далі on-line засоби фільтрації. На уроках, присвячених вивченню служб Інтернету, учитель може так само скористатися засобами контентної фільтрації, що надаються такими компаніями як Яндекс і Гугл.

Батькам важливо мати можливість відгородити себе й своїх дітей від сайтів з матеріалами «для дорослих» при пошуку в Інтернеті. З 1999 року на Яндексі існує «сімейний пошук», де компанія намагається максимально убезпечити користувачів від появи в результатах пошуку сайтів з «дорослим» змістом як за запитами з неоднозначним тлумаченням, так і за прямими запитами [7].

Багато користувачів бажають, щоб у результатах пошуку не з'являвся зміст тільки для дорослих (особливо, якщо цей комп'ютер використовують діти). Фільтри безпечного пошуку Google дозволяють настроїти браузер так, щоб подібний зміст у результатах пошуку не відображався. Google використовує автоматизовані методи визначення неприйнятного змісту й постійно їх удосконалює, враховуючи відгуки користувачів. Для виявлення змісту сексуального характеру використовуються алгоритми перевірки відразу за кількома параметрами: ключовими словами, посиланнями, зображеннями тощо. І хоча не існує фільтрів, які б працювали бездоганно, використання безпечного пошуку в більшості випадків позбавить від змісту подібного роду [8].

Зазначимо, що в умовах розвитку інформаційного суспільства проблема безпечного і захищеного інформаційного зв'язку розглядається як одна з найактуальніших. Американський Національний науковий фонд (NFS) у серпні 2010 року оголосив про започаткування чотирьох дослідницьких проектів, виконуваних під його егідою і спрямованих на створення надійних і безпечних глобальних мереж [9]. Проекти, на розвиток кожного з яких буде виділено по 8 млн. доларів на три роки, увійдуть в уже існуючу програму «Архітектура Інтернету майбутнього». Передбачається реалізація таких концепцій.

Зорієнтованість на мобільність. Канонічний Інтернет заснований на твердих вузлах, однак нова архітектура повинна припускати, що «мобільність повинна бути скоріше нормою, ніж винятком», звичайно, з урахуванням вимог щодо безпеки.

Перехід до іменованих мереж передавання даних (Named Data Networking). Замість маршрутизації трафіка на основі IP-адрес комп'ютерів, нова архітектура буде зосереджена на транспортуванні фактичних даних, які самі зможуть себе захищати. Патрик Кроулі, учений з університету Вашингтона, Сент-Луїс, вважає, що «цей радикальний крок дозволить якісно ліквідувати надлишковий мережний трафік і забезпечити захищений зв'язок з величезною кількістю мобільних приладів».

Використання хмарності. Така архітектура перетворить Інтернет на глобальну хмарну систему з датацентрів, з'єднаних високошвидкісними, наднадійними й безпечними магістральними мережами.

Реалізація XIA (eXpressive Internet Architecture). Йдеться про вбудовану систему безпеки, завдяки якій користувач, що відвідує сайт або завантажує документ, може бути впевненим, що матеріали законні.

«Багато гарного й розумного втілене в сьогоднішньому Інтернеті, ми постараємося зберегти це, — зазначив Пітер Стінкіст, учений з Університету Карнегі-Мелона, — але деякі його частини ушкоджені настільки, що профілактичні заходи вже не допоможуть».

Висновки

Використання Інтернету в навчальному процесі загальноосвітнього закладу потребує запровадження системи надійного захисту школярів від небажаного контенту. Розглянуті засоби дають змогу на безкоштовних засадах реалізувати мультиплатформений контент-фільтр, який можна використовувати як:

- доповнення до будь-якої фільтрації або як самостійний;
- досить гнучку й просту в налаштуванні систему контентної фільтрації;
- досить надійну контент-фільтрацію небажаного трафіка.

Література

1. *Кремень В.Г.* Інформатизація освіти — провідний напрям підвищення результативності навчального процесу: Відповіді Президента НАПНУ В.Г. Кременя / Василь Григорович Кремень // Комп'ютер у школі та сім'ї. — 2011. — №1. — С. 3–6.
2. Концепція Державної цільової програми впровадження у навчально-виховний процес загальноосвітніх навчальних закладів інформаційно-комунікаційних технологій «Сто відсотків» на період до 2015 року. Затверджено розпорядженням Кабінету Міністрів України від 27 серпня 2010 р. №1722-р.
3. *Ротар О.С.* Проблема впровадження освітньо-виховних ресурсів у навчальних цілях: безпечна робота в мережі інтернет // Педагогічний альманах. — 2011. — Вип. 11. — С. 82. [Електроний ресурс]. — Режим доступу до журналу: http://www.nbuv.gov.ua/portal/soc_gum/pedalm/texts/2011_11/015.pdf.
4. *Дітковська Л.А.* Для кого Інтернет може бути небезпечним — [Електроний ресурс]. — Режим доступу до журналу: http://www.nbuv.gov.ua/e-journals/ITZN/ em3/ content/ 07dladbm.htm..
5. *Грабовський П.П.* Зміст програми навчання з основ інформаційно-комунікаційних технологій для вчителів загальноосвітнього закладу [Електроний ресурс]. — Режим доступу до журналу: http://www.nbuv.gov.ua/e-journals/ITZN/em12/content/09gppeec.htm..
6. *Спірін О.М., Ковальчук В.Н.* Методика забезпечення он-лайн безпеки старшокласників у навчально-виховному процесі школи. ISSN 2076-8184. Інформаційні технології і засоби навчання. — 2011. — №1 (21). [Електроний ресурс]. — Режим доступу до журналу: http://www.journal.iitta.gov.ua http://www.nbuv.gov.ua/e-journals/ITZN/2011_1/Kovalchuk.pdf.
7. Сімейний пошук Яндекс [Електроний ресурс]. — Режим доступу: http://family.yandex.ua/.
8. Налаштування безпечного пошуку Google [Електроний ресурс]. — Режим доступу: http://www.google.com/preferences.
9. NSF Announces Future Internet Architecture Awards (Press Release 10-156) [Електроний ресурс]. — Режим доступу: http://nsf.gov/news/news_summ.jsp?cntn_id=117611.