З.С. Сейдаметова
Кримський державний
індустріально-педагогічний інститут

Технологія Cookie: методика вивчення

Підготовка вчителів інформатики передбачає ознайомлення їх із найостаннішими технологічними новинками. Частина учнів зможє дізнаватися про ці новинки від своїх учителів, а знайдуться і такі, котрі почерпнуть цю інформацію з інших джерел, включаючи Інтернет-ресурси – вчитель інформатики не може відставати від своїх найбільш підготовлених учнів.

На сьогоднішній день існує безліч різних Інтернет-технологій. Одна з них – це технологія «Cookie». Вона пронизує весь Інтернет, перетворюючи Всесвітню Мережу в середовище з пам'яттю і можливістю контролю. Технологія «Cookie» – з одного боку сила Інтернету, а з іншого – його слабкість.

1. Історія появи технології. Якось у червні 1994 року, Луї Монтуллі (Lou Montulli) [1] сидів за своїм комп'ютером і намагався удосконалити свою роботу в Інтернеті, зробити її більш зручною. В результаті цієї спроби і народилася нова технологія. До цього моменту в історії Інтернету при повторному відвідуванні сайта необхідно було проробити всі необхідні маніпуляції заново, оскільки сайт не пам'ятав попереднього вашого відвідування. А це було так незручно, якщо раптом вам доводилося перериватися під час сеансу при розриві зв'язку, і повторне з'єднання не дозволяло продовжувати вже почату роботу, доводилося усе починати заново. Навіть не можна було побачити, які гіперпосилання ви вже пройшли. Великі незручності були і при комерційних транзакції. Якщо раптом під час транзакції переривався зв'язок, а ви не встигли дійти до кінця процедури реєстрації, то доводилося усе починати спочатку, проходячи від одного гіперпосилання до іншого і так до кінця. Якщо спробувати пояснити це більш образно, то можна порівняти з раптовою амнезією в магазині при купівлі необхідних продуктів.

У свої 24 роки Луї Монтуллі був співробітником Netscape Communications, і був уже відомий як програміст із видатними здібностями. Замислившись над проблемою запам'ятовування сторінок Інтернету, він швидко знайшов розв'язок, оформивши його у вигляді п'ятисторінкового документу. У цьому документі він докладно описав знайдену ним технологію.

У цьому документі він пропонував, щоб кожен сайт сервера записував у кожен комп'ютер відвідувача невеликий файл з інформацією про те, що робив даний відвідувач на цьому сайті. Луї Монтеллі назвав таку технологію «Постійне спостереження за станом клієнта» («Persistent client state object»). Але була в нього в думках і інша назва, що багато років тому використовувалася програмістами. Ще в перших комп'ютерах для ідентифікації програмісти передавали невеликі двійкові коди. Цей обмін бітами інформації вони називали «Magic Cookies» (чарівні печива). Вважаючи свій винахід прямим нащадком «Magic Cookies», Луї перейменував свою технологію в «Cookie».

Це був поворотний пункт в історії компьютінга. Технологія Cookie перетворила Всесвітню Мережу з місця переривчастих, не спадкоємних відвідувань у середовище з новим додатковим виміром, що має пам'ять. Ця технологія мала велике майбутнє. Cookie можно було використовувати в Інтернет-купівлях, Інтернет-іграх. Ця технологія істотно змінила характер серфінгу. Інтернет перетворився із середовища з анонімною діяльністю клієнтів у середовище, у якій можна було робити угоди, фіксувати себе на сайтах.

З тих пір Cookie стала всюдисущою, вона пронизала всю мережу Інтернет. Опитування американців наприкінці серпня 2001 року показало, що 67% американців вважали мережеву ідентифікацію більш важливою проблемою, ніж злочинність (55%) і протиракетна оборона (22%) (дане опитування проводилося до 11 вересня 2001 року, скоріше усього, після 11 вересня американці мають вже іншу думку). У той же час, у деяких містах США почав зростати гнів громадян з приводу вторгнення в їхнє особисте життя. Громадяни стали закликати до обмеження використання Cookie і інших засобів high-tech, що контролюють дії користувачів Інтернет.

Таким чином, завдяки Cookie клієнт Інтернет-магазину при необхідності може переривати процес заповнення свого кошика замовлень, а потім продовжити цей процес. При поверненні до закупівель сервер сайта запитає клієнта, чи має він бажання завершити своє незакінчене попереднє замовлення. Cookie дозволяє також показувати рекламу, орієнтовану на інтереси кожного клієнта. Звичайно, усе це можливо тільки завдяки персональному ідентифікатору в невеликому файлі cookie на комп'ютері клієнта. Є і зворотний бік цих принадностей і зручностей. Якщо власник веб-сайта зможе об'єднати ідентифікатор з персональною інформацією клієнта і дані про зареєстрованих відвідувачів сайта, то Cookie стає могутнім механізмом для персонального стеження.

Історію виникнення технології Cookie можна закінчити словами Лоуренса Лессіга (Lawrence Lessig), професора Стенфордской юридичної школи, фахівця з питань взаємодії софта і суспільної політики: «До появи Cookie Інтернет був, власне кажучи, приватною мережею. Після появи Cookie Інтернет перетворився у простір з можливістю надмірного контролю» («Before cookies, the Web was essentially private. After cookies, the Web becomes a space capable of extraordinary monitoring»).

2. Патент № 5960411 «Метод і система розміщення замовлення через комунікаційні мережі». У вересні 1999 року компанія Amazon.com (http://www.amazon.com)одержала патент № 5960411 на винахід за назвою «Метод і система для розміщення замовлення через комунікаційні мережі» [2]. У статті [3] розповідається про цей патент як про спробу Amazon монополізувати один з видів електронного бізнесу, а також про прецедент, що дозволяє патентувати ідеї, видаючи їх за

механізми і системи. Ми ж подивимося на патент № 5960411 з чисто технічної сторони, оскільки нас цікавить технологія «cookie», а не електронна торгівля.

Як відомо, Amazon.com – це найбільший інтернет-магазин і цілком логічно, що даний винахід пов'язаний із клієнтською і серверною частинами оформлення замовлення-закупівлі у віртуальному магазині. Відповідно до патентного права США не можна патентувати алгоритми. Тому представники Amazon.com зробили витончений обхідний маневр, запатентувавши не алгоритм, а «метод і систему» віртуального продажу. Запатентований метод, а, швидше за усе все-таки алгоритм, полягає ось у чому.

У текст HTML-документу, що бачить клієнт у вікні броузера, вставляється програмний код, за допомогою якого броузер записує у файл, що знаходиться в комп'ютері клієнта, деяку інформацію чи запише сам файл з інформацією в деяку папку. Потім цю інформацію (при необхідності) можна буде прочитати за допомогою того ж броузера і додати в інформаційний пакет, що буде посланий на web-сервер. Як ви, напевно, уже помітили, цей механізм дуже нагадує «cookie». Цей механізм ілюструється схемою 1.

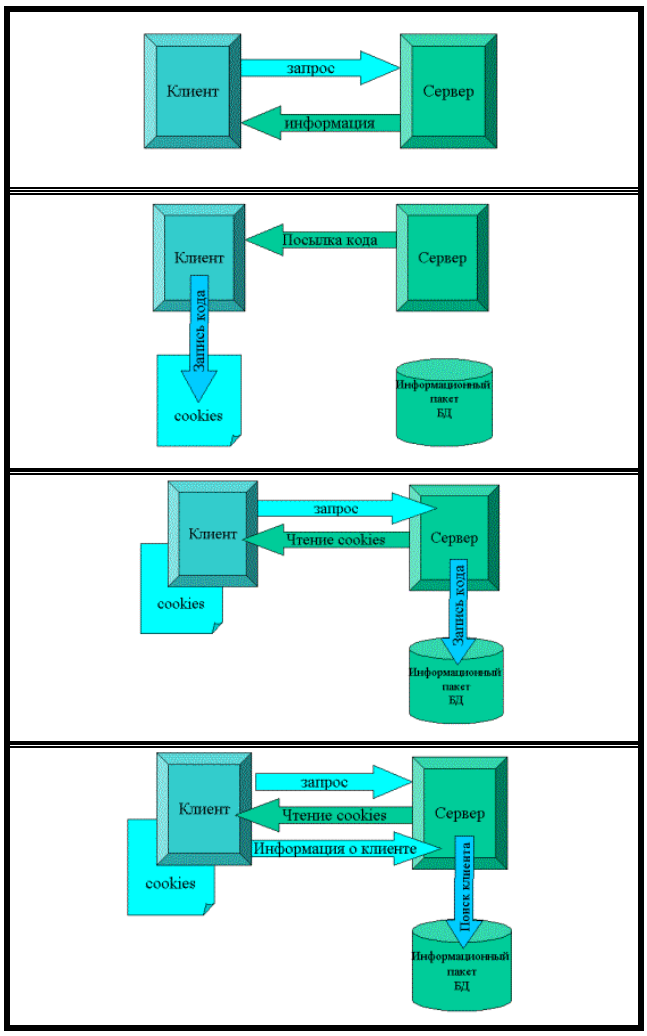


Схема 1. Клієнт-серверний обмін інформацією в технології cookie.

Таким чином, при відвідуванні інтернет-магазину, після того, як клієнт уперше вибрав необхідний йому товар, йому привласнюється унікальний номер, що запам'ятовується у файл cookies.txt (у Netscape Navigator) чи папку Cookies (у IE). Потім при формуванні усіх веб-сторінок даного клієнта ідентифікатор буде додаватися сервером до всіх посилань, що використовуються для навігації по серверу. Працююча під управлінням веб-сервера, програма-скріпт, що розташовується на сервері, виділяє цей ідентифікатор з інформаційного пакета, що у свою чергу формується під час «кліка» на посиланні. Далі в базі даних зберігається інформація про всіх потенційних покупців, їхніх купівлях, смаках і т.п. Оскільки cookies знаходиться на комп'ютері клієнта, при черговому відвідуванні про нього довідаються і будуть формувати для нього усі веб-сторінки з унікальним ідентифікатором. Це дозволяє інтернет-магазинам збирати статистику про кожного свого клієнта індивідуально.

Основу запатентованого методу складає система «One-Click Commerce», зміст якої полягає у внесенні в усі посилання документів веб-сайта унікального ідентифікатора клієнта, що дозволяє згодом визначати автора клієнтського запиту.

3. Cookies і персональна безпека користувача. Восени 2000 року найбільший Інтернет-провайдер США компанія Earthlink провела спеціальну акцію. Учасники акції роздавали десяткам тисяч перехожих шоколадні печива, з написом на упакуванні «чи Відомо Вам, звідки прибувають Cookies?» [4]. Під час цієї акції Earthlink порівнювала свою власну політику захисту прав власності з

політикою лідера індустрії Інтернет-послуг America Online (AOL), і запропонувала своїм клієнтам поради про те, як контролювати Cookies.

Віце-президент з маркетингу компанії Earthlink Клаудіа Каплан сказала: «Наша позиція — пояснити клієнтам, які файли розповідають про них і як ними можна управляти». Компанія Earthlink також запропонувала своїм клієнтам програмне забезпечення, що дозволяє приймати чи відмовлятися від Cookies для збереження своїх таємниць (privacy).

Завдяки проведеній акції вже до літа 2001 року компанія Earthlink змогла збільшити свою частку на ринку з 15% до 25% користувачів.

К. Каплан вважає, що основний компонент такого успіху полягає в тому, що Earthlink поважає privacy своїх клієнтів. Можливо воно і так, але зберігати privacy хоче більшість, але не всі хочуть за це платити. Така думка багатьох користувачів Мережі не тільки у нас, але й у багатій Америці.

Проблема збереження privacy користувачів Інтернет цікавить також і інші компанії. Так, канадська компанія «Zero-Knowledge Systems» запропонувала своїм клієнтам повний набір інструментарію для захисту privacy, назвавши цей програмний продукт «Freedom». Користувачі можуть використовувати це програмне забезпечення для вибіркового блокування Cookies, які веб-сайти намагаються записати на власні комп'ютери і спокійно здійснювати серфінг під вигаданими іменами.

Однак зараз дуже мало людей, що піклуються про своє privacy. Вони плавають по просторах Всесвітньої Мережі і зовсім не думають про збереження таємності. Тому можна констатувати, що поки ще мало покупців такого програмного забезпечення, що зберігає privacy. Алан Вестин, експерт з privacy, вважає, що поки Інтернет-цивілізація така, що середній користувач Мережі працює цілком «розкритим», зовсім не думаючи про збереження таємності. Він також відзначає, що в історії західної цивілізації таке відношення до захисту власної privacy, судячи з усього, спостерігається вперше.

Бізнесмени намагаються зрозуміти небажання користувачів Інтернету захищати своє privacy. У квітні 2001 року компанія WebSide Story вивчили Інтернет трафік 150 тисяч сайтів. У їхньому звіті було відзначено, що тільки 1% відвідувачів сайтів відмовляються від Cookies. На підставі чого був зроблений висновок, що «Cookies просто не турбують користувачів».

Але все-таки реальні причини цього явища – багатогранні. Одна з них – не всі користувачі знають про Cookies, і не усі уміють від них відмовлятися. А іноді від них неможливо відмовитися, сайти вимагають включення Cookies.

Американці завжди піклувалися про збереження власних секретів. Протягом кількох років проводилися публічні дебати з питань Internet-privacy. В результаті проведених опитувань з'ясувалося, що 56% взагалі не розуміли про що йде мова, причому третина з них провела в Інтернеті чимало часу.

Технологія Cookie дозволяє знизити рекламний тиск на відвідувача мережі [5].

У теперішніх умовах економічного спаду IT-індустрії веб-видавництва намагаються різноманітити механізми організації інтернет-реклами, оптімізуючи розмір, форму сторінок, а також засоби доставки онлайнових оголошень. Враховуючи те, що в основному клієнти не люблять витрачати свій час на перегляд реклами, видавництво Salon запровадило зовсім новий формат показу своєї реклами. Завдяки технології cookies вони зможуть тепер демонструвати своїм читачам рекламні оголошення тільки один раз у день. Але це буде можливо тільки в тому випадку, якщо в броузері функція cookies не буде відключена, оскільки в іншому випадку лічильник показів просто не працює.

Технологія Cookie привернула увагу законодавців деяких країн. Так, у листопаді 2001 року Європейський парламент вніс у проект директиви з електронного збирання даних і захисту прав особистості виправлення, яке обмежує використання cookies [6]. Відповідно до цього виправлення, веб-сайти повинні будуть явно запитувати користувачів, чи згодні вони на запис cookies. Можливо, це виправлення виявиться згубним для індустрії інтернет-реклами.

Захисники прав споживачів давно критикували cookies за уразливість у технічному плані і потенційні проблеми privacy у випадку, якщо зламається захист комп'ютера. Лють правозахисників викликає також і той факт, що cookies можуть зберігати дані про діяльність користувачів в Інтернеті за декілька років.

Організація Interactive Advertising Bureau (IAB) попередила, що у випадку ратифікації цієї директиви британські компанії можуть втратити 270 млн. доларів. Представник IAB заявив: «Члени Європарламенту посилаються на закони про захист інформації і Privacy, але cookies лише зберігають інформацію про комп'ютер. Якщо ви використовуєте cookies для пошуку персональних даних, то ці дії і так заборонені існуючими законами». На його думку, для користувачів життя без cookies буде незручним. «Їх і так можна відключити в броузері, але без cookies, якщо ви увійдете на Amazon.com і надаєте переваги, при наступному візиті цю процедуру доведеться повторити».

4. Броузер як центр управління Cookies. Місце, у якому може бути захищена privacy користувача – це Інтернет-броузер. Ранні версії броузерів приймали cookies за замовчуванням. А той, хто хотів забезпечити собі таємність, повинний був змінювати параметри настроювання.

Зараз компанії, що займаються розробкою броузерів, намагаються при проектуванні свого програмного забезпечення врахувати смаки своїх клієнтів, що не люблять cookies, а також і не скривдити залежні від cookies Інтернет компанії, що роблять сервісні послуги.

Netscape Navigator. В даний час Cookie підтримуються – Netscape Navigator 2.0 і більш пізніми версіями. Користувачі Windows можуть побачити cookie у файлі `cookies.txt`, розташованому в директорії `C:\Programs\Netscape\Navigator`, користувачі Macintosh – в системному каталозі під пунктом `Preferences:Netscape`.

Internet Explorer. Internet Explorer почав підтримувати технологію “Cookie” з версії 3.0. У Internet Explorer 6 існують розширені засоби для роботи з файлами cookie, призначені для захисту

приватної інформації.

Останні версії Netscape Navigator і Internet Explorer можуть виводити попередження користувачеві щоразу, коли сервер посилає броузеру cookie. Якщо ви включили це попередження, то передбачена можливість відмовлення від cookie.

Недолік цієї схеми полягає в тому, що багато серверів будуть пропонувати cookie при кожному новому з'єднанні, навіть після того, як ви відмовилися від прийому cookie перший раз. Netscape Navigator 4.0 надає нову можливість – відмовлятися від прийому cookie, що належить не тому вузлу, на якому знаходиться головна сторінка, яка переглядається вами. Це відтинає більшість схем, подібних DoubleClick.

По суті, cookie опрацьовується будь-яким сучасним броузером, у всякому разі їх можна дозволяти чи забороняти глобально або вибірково, так сказати, "за фактом". Жоден з цих механізмів не є дійсно зручним і універсальним, тому більшість користувачів просто дозволяють cookie на усі випадки.

Уперше подібні засоби з'явилися в спеціальному випуску Internet Explorer 5.5, однак у шостій версії вони набули найбільш завершеної форми. Ідея полягає в тому, що в кожному сайті, в якому використовується cookie, повинна бути описана (у XML чи спеціальній компактній формі) політика, якої потрібно дотримуватися при збиранні і наступному опрацюванні даних, у тому числі – можливі міри відповідальності власників сайта за порушення власних зобов'язань. Ця "політика" буде інтерпретуватися броузером, і в залежності від його настроювань чи миттєвого рішення користувача в кожному конкретному випадку механізми cookie можуть дозволятися, заборонятися чи обмежуватися.

Керівник підрозділу Internet Explorer фірми Microsoft Мічел Уолент [7] помітив, що ранні версії їхнього продукту стосовно cookies були націлені на підготовлених користувачів («просунутих юзерів»). Але оскільки число користувачів Інтернет незмінно зростає і не кожен користувач досить підготовлений у питаннях настроювання програмного забезпечення, то програмний продукт повинен бути простим у використанні. Тому наприкінці літа 2001 року компанія Microsoft оголосила про нову технологію P3P [8]. Ця технологія використовується в Internet Explorer 6, а також включена до операційної системи Windows XP. Дана технологія буде забезпечувати безпеку автоматично, за допомогою інструментальних засобів користувачі Інтернет зможуть легко блокувати сайти з нецікавим для них змістом.

Власне кажучи група розробників винайшла мову для повідомлення комп'ютера про політику безпеки користувача без його втручання. Користувачеві необхідно тільки ввести свої критерії щодо захисту таємності, а програмне забезпечення технології P3P буде порівнювати стандарти користувача з політикою кожного сайта і попереджати користувача про можливі конфлікти. Уперше програмне забезпечення, не запитуючи користувача, буде відхиляти cookies автоматично, якщо користувач не змінить параметри настроювання своїх переваг.

Однак, незважаючи на всі переваги технології P3P, що використовується в IE6, аналітики стверджують, що користувачам ще довго доведеться звикати до цієї технології, і не вірять, що P3P зможе істотно розрізняти інформацію, яку буде надавати користувачеві.

5. Як відмовитися від Cookies. Сучасні версії популярних Інтернет-броузерів дозволяють користувачам установлювати cookies чи відмовлятися від cookies [9, 10]. Нижче описано, як можна відмовитися від cookies у різних версіях броузерів Internet Explorer і Netscape Navigator.

Настроювання "cookie" – опції для Internet Explorer 5.x:

- у головному меню вибрати “Сервіс” (“Tools”);
- знайти пункт “Властивості оглядача” (“Internet Options…”);
- знайти закладку ‘Безпека” (“Security”);
- пересуваючи кнопку, вибрати рівень безпеки: “Високий”(“High”), “Середній”(“Medium”), “Нижче середнього”(“Medium-low)”, “Низький”(“Low”) (рис.1);
- чи вибрати “Інший” (“Custom”) рівень, потім прокрутити до розділу “Файли cookie” (“Cookies”) і в установці “Дозволити використання під час сеансу файлів “cookie” (з мережі)” (в англійському варіанті — Set “Allow per-session cookies” to “Enable” or “Disable”) чи в установці “Дозволити використання “cookie”, що зберігаються на вашому комп'ютері” (в англійському варіанті — Set “Allow cookie that are stored on your computer” to “Enable” or “Disable”) увімкнути чи вимкнути кнопку (рис.2):
  - відключити;
  - запропонувати;
  - дозволити;
- натиснути кнопку OK.

Настроювання " cookie"-опції для Netscape Navigator 4.x:

- вибрати у заголовку вікна пункт “Виправлення” (“Edit”);
- знайти пункт “Настроювання” (“Preferences”);
- знайти розділ “Додатково” (“Advanced”);
- у діалоговому вікні “Файли cookies” (“Cookies”) увімкнути кнопку проти пунктів “Приймати усі файли cookies” (“Accept all cookies”) чи “Приймати тільки з вказуванням на викликаючий сервер” (“Accept only cookies that get sent back to the originating server”);
- для відключення cookies вибрати: “Відключити cookie” (“Disable cookie”);
- щоб файли cookie попадали на комп'ютер користувача з відома власника, необхідно знайти “Попереджати про прийняття cookie” (“Warn me before accepting a cookie”) і вибрати “Допускати всі cookie” (“Accept all cookies”) або “Приймати тільки ті, які вказують на „зухвалий” сервер”

(“Accept only cookies that get sent back to the originating server”);

- натиснути кнопку OK.

Настроювання "cookie"-опції для Internet Explorer 6:

- вибрати закладку “Privacy з меню “Tools|Internet Options”;
- вибрати за допомогою лінійки прокручування один із шести рівнів мережної анонімності (рис.3):
    - Accept all cookies (приймати всі cookies);
    - Low;
    - Medium;
    - Medium High;
    - High;
    - Block all cookies (блокувати всі cookies);
- можливе управління аспектами мережної безпеки на закладці “Advanced” (рис.4). Як тільки IE робить блокування cookies, у нижньому правому куті броузера з'являється значок Privacy Report, двічі клацнувши на який (чи вибравши в меню View однойменний пункт), можна довідатися про те, з яких сайтів були опрацьованні cookies, які з них заблоковані, а також персоналізувати опрацювання cookies для окремих Web-сайтів.

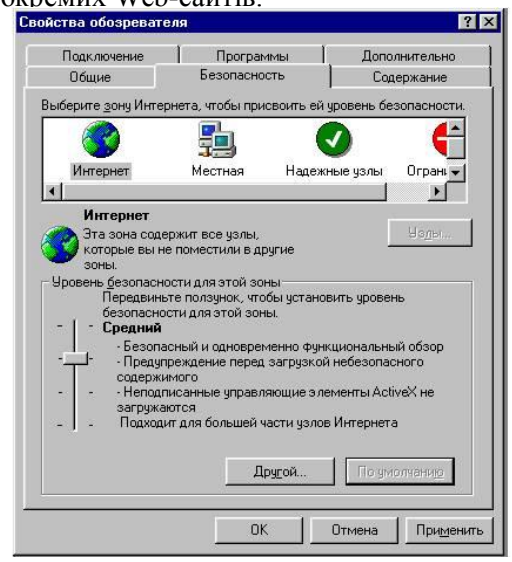


Рис. 1. Настроювання "cookie"-опції для Internet Explorer 5.x

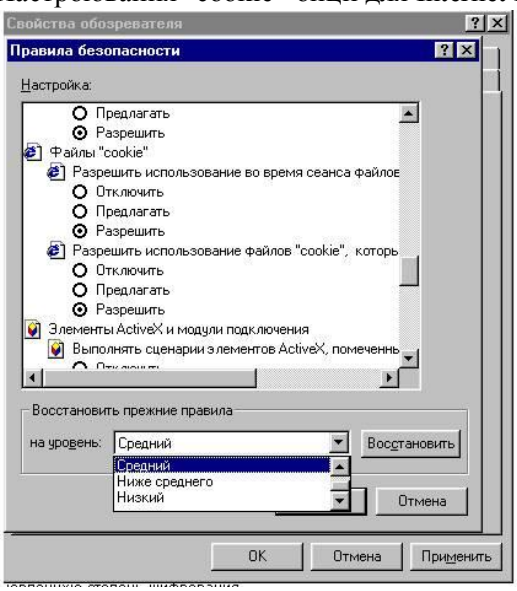


Рис. 2. Настроювання "cookie"-опції для Internet Explorer 5.x

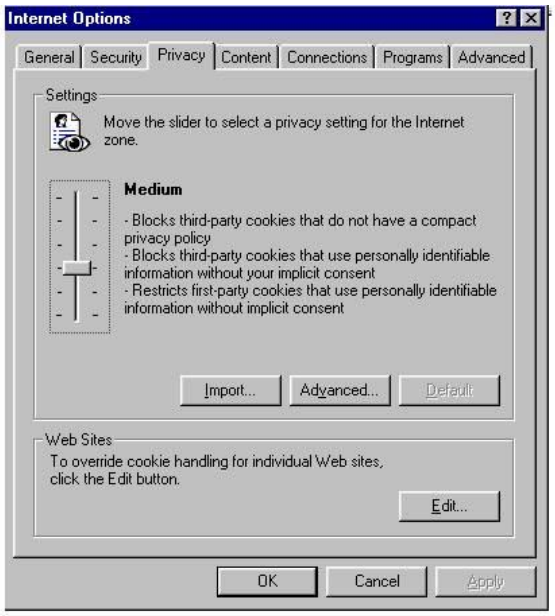
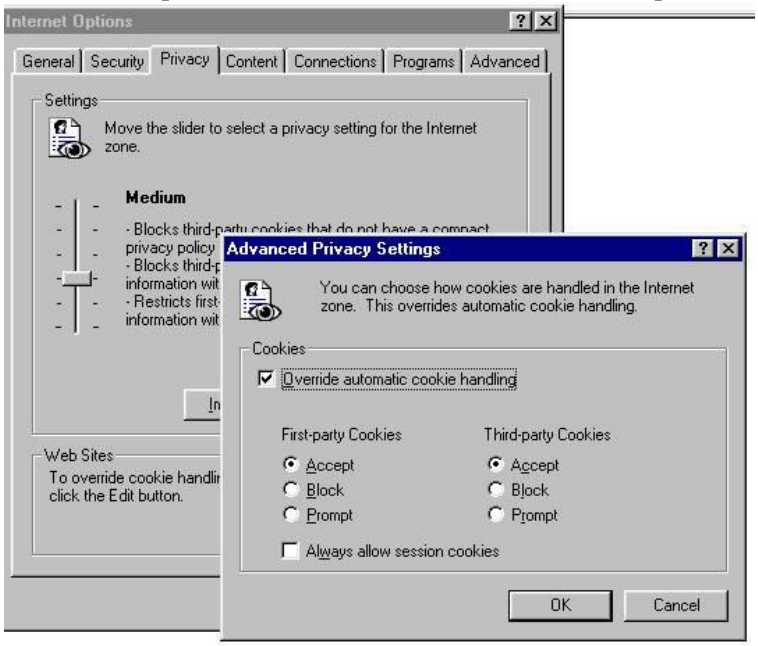


Рис. 3. Настроювання "cookie"-опції для Internet Explorer 6



Мал. 4. Настроювання "cookie"-опції для Internet Explorer 6

6. Три головних питання стосовно Cookies.

1. Чи можна одержати вірус через cookie?

Звичайно, ні. Представники Netscape і Microsoft запевняють користувачів у неможливості одержання вірусу через cookie. Cookie сама по собі нічого не робить. Це просто текстова інформація, що, у свою чергу, є важливим джерелом інформації про відвідувача для сервера.

2. Чи треба боятися cookies?

Боятися cookie не слід. Використовуючи її, неможливо довідатися про ваші персональні дані. Технологія не розрахована на це. Бази даних на серверах одержані не через cookies, а шляхом анкетування клієнтів під час сеансів. До того ж завжди можна відмовитися від cookies чи взагалі їх стерти.

3. Чи можна управляти прийомом cookies?

Існують спеціальні утілити, наприклад, Cookie Manager, Cookie Cruncher для управління прийомом cookie.

7. Формат, синтаксис, способи задання Cookies [11]. **Одержання значень Cookie-наборів.** Імена і значення cookie-наборів встановлюються і зберігаються за допомогою властивості cookie– об'єкта Document. Для збереження неформатованного рядка cookie як змінної необхідно скористатися наступною командою:

var myCookie=document.cookie

Для відображення її на Web-сайті застосовується наступна команда:

*document.write ("Raw Cookies: " + document.cookie + "
");*

JavaScript зберігає cookie-набори в наступному форматі:

Name1=value1; Name2=value2; Name3=value3

Окремі пари NAME=VALUE розділяються крапкою з комою чи пропуском. Після останнього

значення крапка з комою не ставиться. Процес висновку cookie-набору спрощується за рахунок використання програми GetCookie, лістинг якої подано нижче.

```
function GetCookie (name) {
var result=null;
var myCookie= " " + document.cookie + ";";
var searchName= " " + name + "=";
var startOfCookie =
myCookie.indexOf(searchName);
var endOfCookie;
if (startOfCookie != -1) {
startOfCookie += searchName.length;
       // пропустити останнє ім'я cookie
endOfCookie = myCookie.indexOf(";",startOfCookie)
result =
unescape(myCookie.substring(startOfCookie, endOfCookie));
}
return result;
}
```

У даному лістингу рядок myCookie допомагає уникнути обмежуючих умов, при цьому обов'язково треба врахувати, що всі рядкові імена cookie-наборів починаються з пропуску, а закінчуються крапкою з комою. Завдяки цьому не так важко відшукати початок рядка name=, пропустити його і вивести усе, що розташовано між крапкою і наступною крапкою з комою.

8. Встановлення значень Cookie-наборів [12, 13]. Мінімальний опис встановлення значень Cookie-наборів поля Set-Cookie здійснюється за допомогою параметра Name:

Set-Cookie: NAME=VALUE;

NAME=VALUE – рядок символів, що виключає переведення рядка, коми, двокрапки і пробіли. NAME – ім'я cookie, VALUE – значення. У цій комбінації знаходиться мінімальний обсяг інформації, необхідний для встановлення cookie-набору. Однак, є ще параметри, необхідні для cookie. Повний список параметрів, застосовуваних для специфікації cookie-набору наступний:

- name=value
- expires=date
- path=path
- domain=domain_name
- secure

Name і value можуть бути будь-якими. Наприклад, FavoriteColor=Blue чи CurStat=1:2:1:0:0:1:0:3:1:1.

Найпростіший вид для встановлення cookie-набору наступний:

```
function SetCookieEZ (name, value) {
document.cookie = name + "=" + escape(value);
}
```

У цій формі будь-яке нове ім'я (name) додається до активного списку cookie-наборів. Якщо ім'я вже було присвоєне, первісно присвоєне ім'я замінюється останнім. Але існують і виключення, які можна реалізовувати за допомогою параметра path.

Параметр expires=date інформує броузер про час існування cookie-набору. Наприклад, розглянемо формат, заснований на Internet RFC 822

```
Expires = Mon, 04-Feb-2002 05:18:24 GTM
```

Після закінчення встановленої дати cookie перестає зберігатися. Якщо ж цей параметр не встановлений, то cookie зберігається до закриття броузера.

Наступний фрагмент коду встановлює дату закінчення cookie-набору через тиждень.

```
var name="foo";
var value="bar";
var oneWeek = 7 * 24 * 60 * 60 * 1000;
var expDate = new Date ();
expDate.setTime (expDate.getTime () + oneWeek);
document.cookie = name + "=" + escape(value) +
"; expires=" + exp.Date.toGMTString ();
```

У даному фрагменті використана функція toGMTString( ), за допомогою якої можна встановити термін закінчення дії cookie-набору (GMT – Greenwich Mean Time).

Path=path – за допомогою цього параметра встановлюють підмножину каталогів, для якої дійсне значення cookie-наборів. Нижче наведено три приклади створення cookie-наборів за допомогою атрибута path.

Приклад 1.

```
document.cookie="foo=bar; path=/windows";
```

У цьому прикладі cookie-набір foo доступний на кожній сторінці в каталозі windows та його підкаталогах.

Приклад 2.

```
document.cookie="foo=bar; path=/windows/cookies";
```

Тут cookie-набір foo доступний сторінкам у каталозі /windows/cookies, але не буде доступний сторінкам у каталозі /windows.

Приклад 3.

```
document.cookie="foo=bar; path=/";
```

Тут cookie-набір foo доступний кожній сторінці на всьому сервері.

Domain=domain_name – встановлює на даному сайті доступ до інших Web-серверів.

Можна згенерувати такий cookie-набір, щоб всі Інтернет-користувачі змогли його побачити. Розроблювач може тільки встановити шлях всередині домена, оскільки застосування атрибута domain передбачає використання, як мінімум, двох періодів доменних імен, якщо ваш домен завершується на `.com, .edu, .net, .org, .gov, .mil, .int` (наприклад, .yahoo.com). У протилежному випадку повинні бути наявними хоча б три крапки.

Якщо цей параметр опущений, то за замовчуванням використовується доменне ім'я сервера, на якому задане значення cookie-набору.

Secure – повідомляє броузеру про те, що даний cookie-набір повинен відправлятися тільки за умови безпечного з'єднання із сервером у захищеному режимі HTTPS (HTTPS –протокол передавання зашифрованої інформації через Інтернет).

Якщо параметр secure відсутній, cookie-набір пересилається звичайним способом.

Коли запитується документ із http-сервера, броузер перевіряє, чи відповідають наявні cookie-набори домену сервера та іншої інформації. Якщо ці параметри збігаються, броузер надсилає їх до сервера у вигляді:

```
Cookie: Name=value;
```

9. Переваги, обмеження і проблеми, пов'язані з використанням Cookies. Однією з основних переваг cookie-наборів є їхня стійкість. Якщо броузер клієнта настроєний на прийом cookie, то ці набори зберігаються досить довго. Завдяки цьому зберігається інформація про останні відвідування клієнта. Властивість стійкості забезпечує доступ до cookie щоразу, коли клієнт повертається на сторінку.

Треба пам'ятати, що є певні обмеження. Звичайно cookie-набори зберігаються на комп'ютері клієнта в спеціальному файлі cookie чи каталозі Cookie (у залежності від броузера). Так само, як і інші файли, файл із cookie можна видалити як випадково, так і з визначеною метою. Файл із cookie можна захистити від запису. За допомогою броузера можна накладати обмеження на розмір чи кількість збережених cookie-наборів. Нові cookie-набори можуть перезаписувати інформацію в старих наборах.

Оскільки cookie-набори пов'язані з визначеним типом броузера, при переході клієнта з одного броузера на інший можуть виникнути проблеми. Наприклад, якщо колекція cookie отримана в результаті роботи в Netscape Navigator, то при переході до Internet Explorer доступ до цих cookie буде витрачений.

Проблеми виникають і у випадку, коли кілька людей використовують один і той самий комп'ютер і броузер. У них будуть спільні cookie-набори, оскільки броузер, зберігаючи інформацію у файлі, не відрізняє різних користувачів одного і того ж комп'ютера.

Треба мати на увазі, що не можна встановити необмежену кількість cookie-наборів для броузера. Броузер має певні обмеження:

- кількість cookie на сервер чи домен не перевищує 20;
- броузер може зберігати до 300 значень cookie;
- розмір cookie не може перевищувати 4 Кбайт.

Якщо перші два обмеження не виконуються, то віддаляється перший за часом запис. При перевищенні ліміту 4 Кбайт відрізається частина запису на початку cookie, зберігається остання частина cookie, що відповідає граничному обсягу.

Більш докладну інформацію про cookie можна одержати на сайтах [13, 15, 16, 17, 18].

ЛІТЕРАТУРА

1. John Schwartz. Giving the Web a Memory Cost Its Users Privacy.– The New York Times, September 4, 2001.– http://www.nytimes.com/2001/09/04/technology/04COOK.html
2. № 5960411 «Method and system for placing a purchase order via a communications network». Класс G06F 017/60.– http://www. gnu.org/philosophy/amazonpatent.html
3. Александровский А. «Чудеса Амазона» – «Мир Интернет», № 8 (47), август 2000, http://www.iworld.ru/magazine/ index.phtml?fnct=magazine&m=53060111
4. Schwartz John, As Big PC Brother Watches, Users Encounter Frustration. – The New York Times, September 5, 2001. – http://www.nytimes.com/2001/09/05/technology/05COOK.html
5. Стефани Олсон. Веб-сайты встречают читателей рекламой – http://zdnet.ru/?ID=22891, 26 сентября, 2001.
6. Мэтт Лоуни. Европейский парламент сажает рекламщиков на диету – http://zdnet.ru/?ID=176408 , 14 ноября, 2001.
7. Michael Wallent: “Geeks tend to love knobs; they love to twiddle.” – “The Browser as a Cookie-Control Key”, The New York Times, September 5, 2001.– http://www.nytimes.com/2001/ 09/05/technology/05BROW.html
8. Platform for Privacy Preferences. – http://www.w3.org/P3P/
9. Chami.com – http://www.chami.com/tips/internet/, Netscape navigator, Internet Explorer.
10. How to Say No to Cookies. – The New York Times, September 5, 2001.– http://www.nytimes.com/2001/09/05/technology/ 05COOK-SIDE.html
11. JavaScript. Энциклопедия пользователя: Пер. с англ./Аллен Вайк. – К.: Изд-во «ДиаСофт», 2001. 464 с.
12. Аликберов А. Зачем нужны cookies? – http://audio-video. narod.ru/document/Designer/cookie.htm
13. Аликберов А. Что такое cookies и как с ними работать. – http://friends.pomorsu.ru/citforum/internet/html/cookie.shtml
14. Internet RFC 822. – http://www.w3.org/hypertext/WWW/ Protocols/rfc822/#z28

15. Страница спецификации cookie-наборов компании Netscape. – http://www.netscape.com/newsref/std/cookie_spec.html
16. Броузеры, поддерживающие cookie-наборы. – http://www. research.digital.com/nsl/formtest/stats-by-test/NetscapeCookie. html
17. Центр cookie-наборов. – http://www.cookiecentral.com
18. Robert's Brooks' Cookie Taste Test. – http://www.geocities. com/SoHo/4535/cookie.html