УДК 004.056, 342.721

Козак В.Ф.[1], Гарасим Ю.Р.[2], Дудикевич В.Б.[3], Нечипор В.В.[3]
[1]Державна служба України з питань захисту персональних даних
02660, м. Київ, вул. Марини Раскової, 15
[2]ТзОВ «ІТ Капітал»
відділ інформаційної безпеки
04108, м. Київ, пр-т Свободи, 2
[3]Національний університет «Львівська політехніка»
кафедра «Захист інформації»
79013, м. Львів, вул. С. Бандери, 12

ДОСЛІДЖЕННЯ ВІДКРИТОСТІ ТА ПРОЗОРОСТІ ОБРОБЛЕННЯ ПЕРСОНАЛЬНИХ ДАНИХ В ІНТЕРНЕТІ. ТЕХНОЛОГІЯ WEB TRACKING

© Володимир Козак, Юрій Гарасим, Валерій Дудикевич, Віталій Нечипор, 2013

В статті наводяться результати дослідження відкритості та прозорості оброблення персональних даних в Інтернеті, зокрема факту виявлення використання технології web tracking.

Ключові слова – захист персональних даних, web tracking, cookie, flash cookie, DOM objects.

The paper presents the openness and transparency of personal data processing on the Internet research logical continuation results, including the use of web tracking technology.

Keywords – privacy, data protection, web tracking, cookie, flash cookie, DOM objects.

Вступ

Низький рівень правової культури володільців персональних даних, які здійснюють їх оброблення з використанням веб-ресурсів, коли ігноруються найпростіші вимоги закону при зборі та обробленні персональних даних, зумовлює актуальність дослідження небезпеки для приватного життя користувачів в мережі Інтернет некоректного використання автоматизованих засобів відслідковування особливостей поведінки користувачів Інтернет при відвідуванні веб-сайтів.

Цілком раціональні засоби, що використовуються для забезпечення кращого задоволення споживацьких потреб, за умов надмірного їх використання, надмірного збору відомостей про споживачів, фізичних осіб, які за певних обставин можуть бути ідентифікованими, можуть зумовити втручання в приватне життя. В країнах Європи цій проблемі надається значної уваги [1].

Для відслідковування особливостей поведінки відвідувачів веб-ресурсів використовуються такі технології:

- надсилання до пристрою користувача cookies першої та cookies третьої сторони;
- збирання в базах веб-ресурсів детальної інформації протягом тривалого часу про відвідані сторінки, вибрані режими, натиснуті клавіші, тощо, та її подальше оброблення;
- збирання в базах веб-ресурсів інформації про апаратні та програмні засоби, які встановлено у користувача тощо.

Ризики порушення приватності при обробці відомостей про уподобання та поведінку відвідувачів веб-ресурсів

Виявлення конкретних випадків оброблення персональних даних за відсутності законних підстав, чи оброблення надмірного складу персональних даних стосовно визначеної мети – досить складне завдання. Проте, існує можливість оцінити міру взаємодії веб-ресурсу з його

користувачами, яку використовуватимемо для мінімізації потенційних ризиків для недоторканності приватного життя в мережі Інтернет (табл. 1) [2].

Поведінка веб-ресурсів є прозорою. Коли користувач звертається до веб-сайту, відповідно сформований HTML код з цього веб-сайту завантажується в браузер користувача. Цей код можливо перевірити, наприклад, за допомогою опції «Перегляд вихідного коду» браузера. За результатами перевірки можливо безпосередньо встановити потенційно небезпечну поведінку веб-сайту щодо збору та оброблення персональних даних, наприклад: використання cookies або інших ідентифікаторів, перенаправлення на інші веб-сайти, що може встановлювати незадекларовані в політиці конфіденційності зв'язки з третіми сторонами [2].

Таблиця 1

Ризики для недоторканності приватного життя в мережі Інтернет

Ризик	**Ідентифікація IP-адреси**
Вплив	Якщо користувач має статичну IP-адресу, вона може бути ідентифікована та відстежена в розрізі кількох сеансів; стосується усіх веб-сторінок, хоча зовнішні сторінки (рекламодавці) можуть не мати користі від такої інформації.
Рішення	Використання proxy-серверів та анонімайзерів (можуть заборонятися окремими внутрішніми політиками інформаційної безпеки компанії).
Ризик	**Cookies**
Вплив	Можливість відслідковувати користувача на декількох веб-сайтах протягом декількох сеансів, або протягом тривалого часу
Рішення	Відключення cookies в налаштуваннях браузера або використання фільтрації на proxy-серверах.
Ризик	**Велика кількість персоналізованої інформації у заголовку** HTTP (наприклад, мова, ОС і версія браузера).
Вплив	Витік такої інформації на стороні веб-серверу.
Рішення	Використання фільтрації на proxy-серверах.
Ризик	**Вбудовані в HTTP cookies та user pinning**
Вплив	Можливе відстеження користувача на декількох сторінках (але не більше ніж в розрізі декількох окремих сеансів).
Рішення	Поки немає. Можливо, контент-фільтрація (складність використання, низька надійність результатів). Інша можливість полягає в тому, щоб заборонити приховані поля в HTML-формах, таким чином, щоб всі дані, які відправляються були доступні користувачу. Це, в свою чергу, може зумовити порушення функціонування окремих веб-сайтів.
Ризик	**Ймовірне завантаження JavaScript з інших веб-сайтів** JavaScript має змогу надати дозвіл серверу для отримання такої інформації, як: локальна IP-адреса (навіть при використанні proxy-сервера), локальну інформацію про конфігурацію тощо.
Вплив	Відстеження користувачів, витік такої інформації, як: ОС, версія браузера, роздільна здатність екрану, плагіни, які використовуються.
Рішення	Відключення JavaScript.
Ризик	**Обмін ідентифікаторами з використанням 302-перенаправлення**
Вплив	Може використовуватися, для обміну cookies або іншими ідентифікаторами користувачів.
Рішення	В деяких випадках відмова від використання cookies

За ініціативи Всеукраїнської громадської організації «Українська асоціація захисту персональних даних» 25 жовтня 2012 року було прийнято [3] Декларацію «За недоторканість приватного життя в Інтернеті» [4], до якої приєдналися низка провідних національних телекомунікаційних компаній [5,6].

Третій Український Форум з Управління Інтернетом (IGF-UA), у своїй Резолюції [7] звернувся до постачальників послуг Інтернет щодо доцільності дотримання рекомендацій Комітету міністрів Ради Європи № R (99) 5 від 23.02.1999 р. державам-членам Ради Європи «Про захист недоторканості приватного життя в Інтернеті» [8].

Українською асоціацією захисту персональних даних ініційовано та проведено перше дослідження в рамках громадського моніторингу відкритості та прозорості оброблення персональних даних в Інтернеті [9].

Виявилося, що серед трьох типових категорій ресурсів національного сегменту мережі Інтернет – інтернет-медіа, інтернет-торгівля та розваги, найбільш відкрито та прозоро оброблення персональних даних здійснюється в сегменті розважальних інтернет-ресурсів.

Лише не більше третини веб-ресурсів надають суспільству та користувачам мінімальні відомості про володільця персональних даних – найменування юридичної чи ім'я фізичної особи, яка і є, відповідно до законодавства, відповідальною за оброблення персональних даних відвідувачів та за дотримання їх прав на невтручання в сімейне та приватне життя, лише не більше третини веб-ресурсів повідомляють відвідувачів про їх права складно заперечувати.

Можна впевнено зробити висновок, що переважна частина національних веб-ресурсів, можливо більше трьох четвертей, не забезпечують відкритості і прозорості оброблення персональних даних, ігнорують вимоги ратифікованої Україною Конвенції про захист осіб у зв'язку з автоматизованим обробленням персональних даних, положень Закону України «Про захист персональних даних», рекомендацій Комітету міністрів Ради Європи № R (99) 5 від 23.02.1999 р. державам-членам Ради Європи «Про захист недоторканості приватного життя в Інтернеті».

За результатами громадського моніторингу забезпечення прозорості та відкритості оброблення персональних даних на веб-ресурсах підготовлено звіт №1 [10], перелік веб-ресурсів різних категорій та виявлені на цих ресурсах ознаки відкритості та прозорості обробки персональних даних наведено в [11].

В дослідженні використовувалися прості методи аналізу описаних явно, або таких, що реалізуються, але не описаних, політик обробки персональних даних. Подальші дослідження спрямовані на вивчення прозорості і відкритості обробки персональних даних при здійсненні збору, обробленні та подальшому зберіганні даних про кінцевих користувачі веб-ресурсів.

Відомості про те, хто та коли відвідував веб-ресурс, які саме сторінки сайту відвідувалися, в якій послідовності, та ін. збирається та, в подальшому, аналізується, на серверах веб-ресурсів, які відвідувалися (перша сторона), та спеціалізованими веб-ресурсами, які здійснють аналітичні дослідження, організовують відображення контекстної реклами, вивчають ефективність такої реклами, тощо (третя сторона).

Слід зазначити, що обробка відомостей про відвідувачів першою стороною, як правило, здійснюється на законних підставах, адже відвідувач, після ознайомлення з політикою обробки персональних даних на цьому веб-ресурсі, надає згоду на обробку його персональних даних. Водночас, передача відомостей про відвідувача для обробки третій стороні, збір та обробка відомостей про відвідувачів веб-ресурсів третіми сторонами не завжди здійснюється відкрито і прозоро, за згодою відвідувача.

Дослідження відкритості та прозорості обробки відомостей про уподобання та особливості поведінки відвідувачів веб-ресурсів має такі особливості:

- лог-файли, накопичені сервером веб-ресурсів першої та третьої сторони (журнали записів про події роботи сервера) для громадського моніторингу не доступні;
- політика веб-ресурсів щодо передачі відомостей про відвідачів третім сторонам, або щодо надання доступу третім сторонам до відомостей про відвідувачів сайту у більшості випадків або відсутня, або не повна, або не відповідає реальним процедурам, що запроваджені. Не виключено, що в багатьох випадках, власники веб-ресурсів не знають, хто і на яких підставах збирає відомості про їх відвідувачів.
- Зважаючи на зазначене, для дослідження можуть використовуватися такі методи, як:

– вивчення наявних елементів політик перших сторін, а також політик третіх сторін;
– вивчення процедур запису відомостей про відвідані сторінки (cookies, flash cookies, DOM Storage files, та ін.) в папки браузера на стороні користувача;
– виявлення та вивчення особливостей функціонування скрипт-файлів третіх сторін на веб-ресурсах перших сторін, результатів їх діяльності та можливі загрози недоторканості приватного життя користувачів ресурсу.

В даній статті наводяться результати дослідження відкритості та прозорості оброблення персональних даних в Інтернеті, зокрема щодо факту виявлення використання технології web tracking.

Технологія cookies

Технологія cookies вже не перший рік перебуває у полі зору фахівців у галузі інформаційної безпеки, і на цей час багато антишпигунських програм містять засоби пошуку шкідливих cookies і значні бази сигнатур для реалізації такого пошуку [12].

Cookies – це текстова інформація невеликого обсягу, яка зберігається на комп'ютері користувача за запитом веб-сервера і віддається йому при повторних відвідуваннях веб-ресурсу. Основним призначенням cookies є:

– організація сесій під час роботи користувача з он-лайн магазинами, банкінгом, форумами та іншими інтерактивними системами з веб-інтерфейсом, наприклад, з системами документообігу або поштовими сервісами. У цьому випадку в cookies зберігаються деякі параметри сесії, зокрема її унікальний ідентифікатор;
– зберігання різних параметрів користувача. Іноді в cookies зберігаються не самі дані, а якийсь ідентифікатор, що дає змогу програмному забезпеченню веб-сервера ідентифікувати користувача;
– ідентифікація користувача в рейтингових системах, лічильниках, системах банерного показу, он-лайн голосуваннях.

Методика зберігання cookies залежить від типу браузера. Наприклад, Internet Explorer зберігає дані cookies у вигляді окремих текстових файлів в особливій папці «Cookies», яка розташована в профілі користувача. Єдиним засобом захисту даної папки є наявність у неї атрибуту «Системний», що робить її невидимою для користувача. Самі ж файли мають розширення *.txt і можуть бути переглянуті за допомогою звичайного текстового блокнота.

Браузер Mozilla Firefox зберігає cookies в профілі користувача – у файлі Application Data\ Mozilla\Firefox\Profiles\<ім'я користувача>\cookies.txt. Цей файл має досить просту структуру: коментарі починаються з символу #, дані cookies розташовуються по одній на кожний рядок, а роздільником полів слугує знак табуляції.

Крім цього cookies беруть участь в таких складних атаках як Cross-Site Request Forgery (CSRF) (восьма позиція згідно OWASP TOP 10) [13].

З cookies пов'язано декілька основних видів загроз:

– витік конфіденційної інформації – може відбутися у випадку отримання зловмисником даних, які зберігаються в cookies будь-яким способом;
– несанкціонований доступ зловмисника до деяких веб-послуг від імені користувача. Це в першу чергу стосується отримання з cookies ідентифікатора сесії, а також збережених в cookies імені та пароля користувача або їхнього еквівалента;
– отримання інформації про те, які вузли відвідувалися користувачем останнім часом. В даному випадку аналіз cookies, разом із журналами браузера і кешем сторінок, дає змогу отримати досить повну картину про вподобання користувача. Такий аналіз зазвичай проводиться фахівцями спецслужб або служби безпеки (forensics).

Типовими способами отримання зловмисниками інформації з cookies є:

Міжсайтовий скриптінг. Найпростіший і популярний метод викрадення cookies, який базується на впровадженні в легітимну веб-сторінку невеликого троянського скрипта, що передає

доступні вузлу cookies зловмисникові. Крім того, з його допомогою існує можливість викрасти сеансові cookies.

Експлуатація вразливостей браузера.

Впровадження на комп'ютер користувача троянської програми, яка аналізує інформацію в cookies і передає її зловмисникові. Крім цього, троянська програма може не лише аналізувати cookies, але і модифікувати їх. Створити таку програму досить просто, оскільки Internet Explorer і Mozilla Firefox зберігають cookies у відкритому вигляді.

Використання комп'ютера в публічних місцях – в бібліотеках Інтернет-кафе тощо. Це пов'язано з тим, що багато користувачів не видаляють журнали роботи та cookies по завершенні роботи.

Перехоплення cookies за допомогою засобів аналізу мережевого трафіку.

Реєстрація даних cookies в протоколі проксі-сервера. Залежно від своїх налаштувань проксі-сервер може здійснювати запис не лише повного URL, але і заголовків HTTP-запиту та відповіді.

Технологія web tracking

Оскільки протокол HTTP (протокол передавання гіпертексту) не зберігає стан запиту кінцевого користувача на сервер і кожен наступний запит є відокремленим від контексту попереднього і позиціонується сервером як унікальний, було створено механізм, що забезпечує ідентифікацію користувача між окремими запитами до сервера. Саме це зумовило виникнення технології web tracking. Для збереження інформації про діяльність користувача веб-ресурси використовують такі основні контейнери даних:

- Cookie,
- Flash Cookie,
- DOM Storage.

Контейнери даних побудовані за принципом «ключ-значення» і можуть бути використані для встановлення унікального ідентифікатора сесії користувача. Серед зазначених контейнерів даних найбільше відрізняється Flash Cookie. Особливість Flash Cookie полягає в тому, що він є спільним для усіх браузерів на комп'ютері користувача та здатен містити більші об'єми даних.

Практично це означає, що наявний на веб-ресурсі скрипт третьої сторони може отримати доступ до cookie і звертатися до них з кожного веб-ресурсу, на якому він присутній (не залежно від браузера, який використовується). При цьому кожному файлу cookie присвоюється унікальний ідентифікатор, який використовується для ідентифікації користувача між запитами на різні веб-ресурси.

Наявність скрипта, який наданий третьою стороною на сторінці веб-ресурсу, що містить форму авторизації або реєстрації користувача означає, що в момент відправлення форми, яка містить, наприклад, адресу електронної скриньки користувача, його логін і/або ім'я, прізвище тощо, які надані користувачем, можуть бути передані третій стороні разом з його унікальним ідентифікатором. Наступного разу, зайшовши на сторонній веб-ресурс, на якому також присутній цей скрипт, третя сторона може мати змогу отримати дані про діяльність користувача на даному ресурсі. Таким чином з'являється можливість відстеження діяльності та автентифікація користувача у мережі Інтернет, що становить пряму загрозу приватності життя.

Методика дослідження

Для дослідження веб-ресурсів України (аналогічно як у моніторингу [11]: три категорії по 20 веб-ресурсів в кожній) використана методика, яка полягає у виявленні факту наявності сторонніх скрипт-файлів, результатів їх діяльності та впливу на кінцевого користувача.

В процесі підготовки до етапу виявлення факту встановлення flash cookie при відвідуванні веб-ресурсу було:

1. дозволено виконання усіх javascript функцій на веб-сторінці;
2. відключено блокування скриптів третьої сторони у додатку до Mozilla Firefox Ghostery;
3. дозволено використання сховища DOM об'єктів у Mozilla Firefox;
4. дозволено встановлення flash cookie в налаштуваннях до macromedia flash плагіна на веб-сторінці
   http://www.macromedia.com/support/documentation/en/flashplayer/help/settings_manager03.html

5. очищено усі встановлені flash cookie.

Сам процес виявлення фактів встановлення flash cookie об'єктів виглядав таким чином:

1. відкриття в браузері Mozilla Firefox досліджуваного веб-ресурсу;
2. перехід по посиланням на самому веб-ресурсі, що зумовлюють перехід до сторінок реєстрації, коментування, заповнення анкет та будь-яких інших розділів веб-ресурсу, де можуть бути зібрані та в подальшому оброблені персональні дані користувача;
3. перевірка встановлених flash cookie;
4. у випадку виявлення факту встановлення flash cookie проводилось виявлення сторонніх javascript вставок, що є відповідальними за це;
5. очищення встановлених flash cookie та перехід до кроку 1 для наступного веб-ресурсу.

Результати дослідження

За результатами дослідження:

– визначено сторонні ресурси, що вбудовують свою функціональність в існуючий функціонал сторінки;
– досліджено flash cookie файли, що встановлюються третіми сторонами;
– досліджено запити, якими обмінюються ресурси з третіми сторонами;
– досліджено дані, які передаються з використанням сторонніх віджетів та скриптів.

Встановлено, що переважна більшість розглянутих веб-ресурсів містить блоки javascript коду, який надається третіми сторонами. Дані javascript функції забезпечують відображення рекламних банерів, віджетів соціальних мереж, а також «share» кнопок, підрахунок відвідуваності сайту.

Для дослідження присутності на вказаних сайтах діяльності третіх сторін, що займаються web tracking було використано додаток Ghostery [14] до браузера Mozilla Firefox.

Даний додаток містить базу більш як з 1300 найпоширеніших веб-ресурсів, які розділені на 5 категорій: 1) реклама, 2) аналітика, 3) трекінг, 4) приватність, 5) віджети.

Частина досліджуваних веб-ресурсів надає можливість авторизації та створення профілю користувача за допомогою використання облікового запису популярних соціальних мереж (рис. 1).

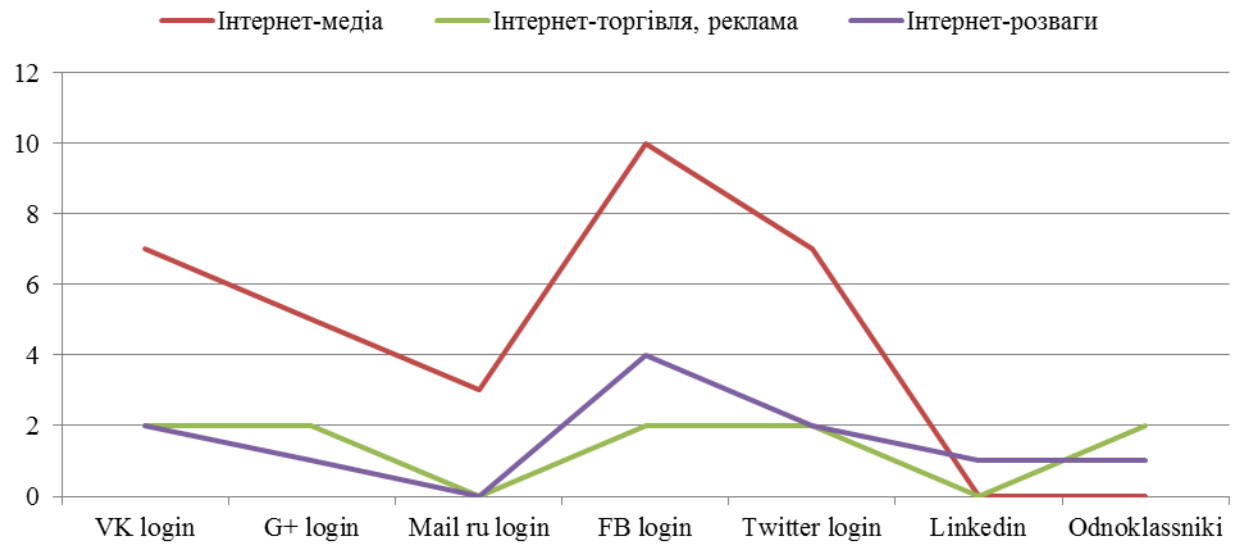

Рис. 1. Популярність використання способу авторизації за допомогою соціальних мереж

Найбільше технологію web tracking використовують веб-ресурси з категорії «Інтернет-медіа» (53%) та «Інтернет-розваги» (31%) (рис. 2). Найчастіше технологію web tracking типу Advertising, Analytics, Beacons, Widgets використовують веб-ресурси з категорії «Інтернет-медіа», а значно рідше веб-ресурси з категорії «Інтернет-торгівля, реклама» (рис. 3). Найпопулярнішою ж технологією web tracking є Advertising та Analytics (рис. 4). Серед технології web tracking типу Advertising найпоширенішими є: bigmir, Adriver, Google Adsense, Gemius (рис. 5), а типу Analytics: bigmir, AdRiver, Google Adsense, Gemius (рис. 6).

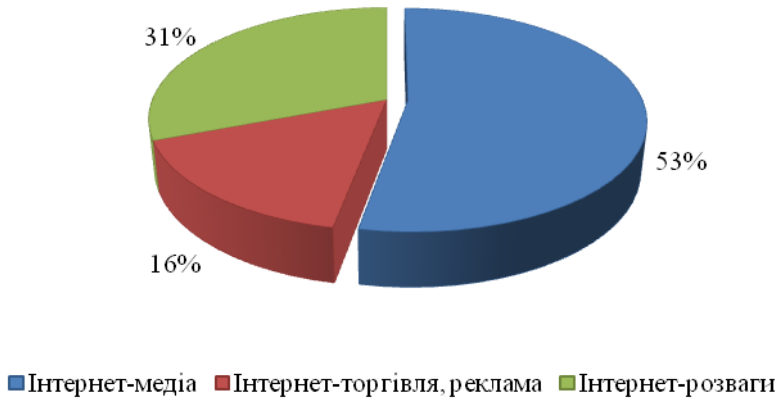

Рис. 2. Використання технології web tracking веб-ресурсами трьох категорій

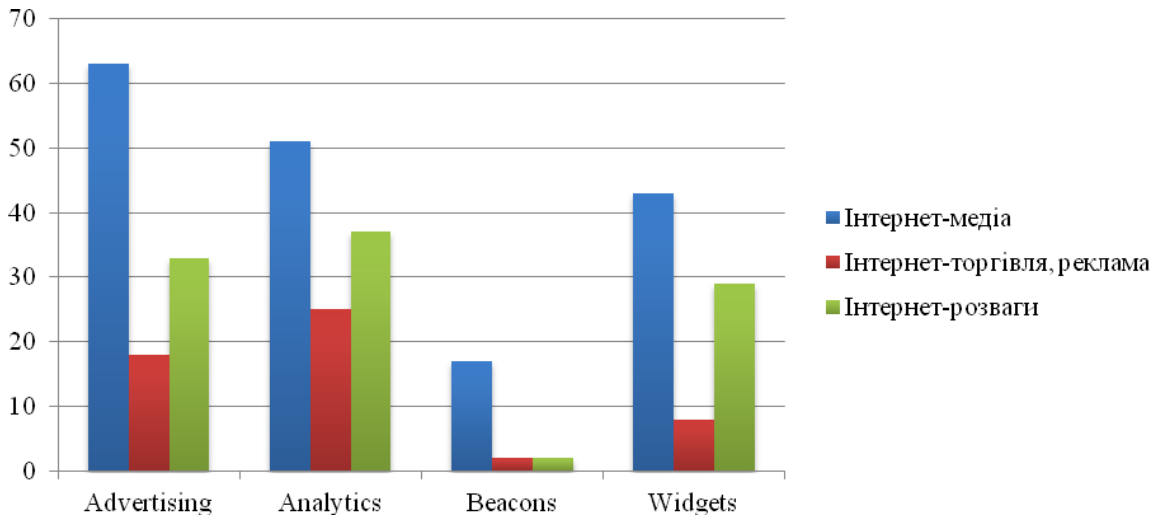

Рис. 3. Типи та кількість технології web tracking, які використовують веб-ресурси трьох категорій

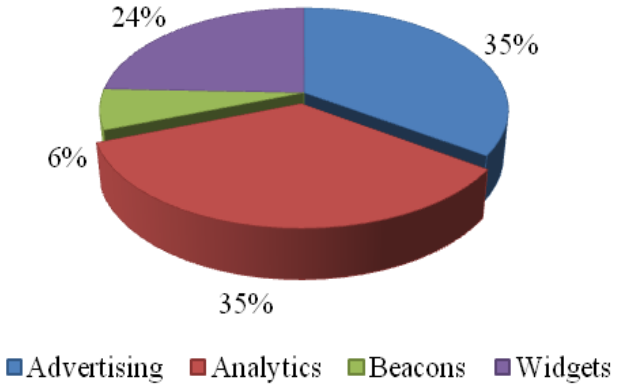

Рис. 4. Популярність використання типів технології web tracking

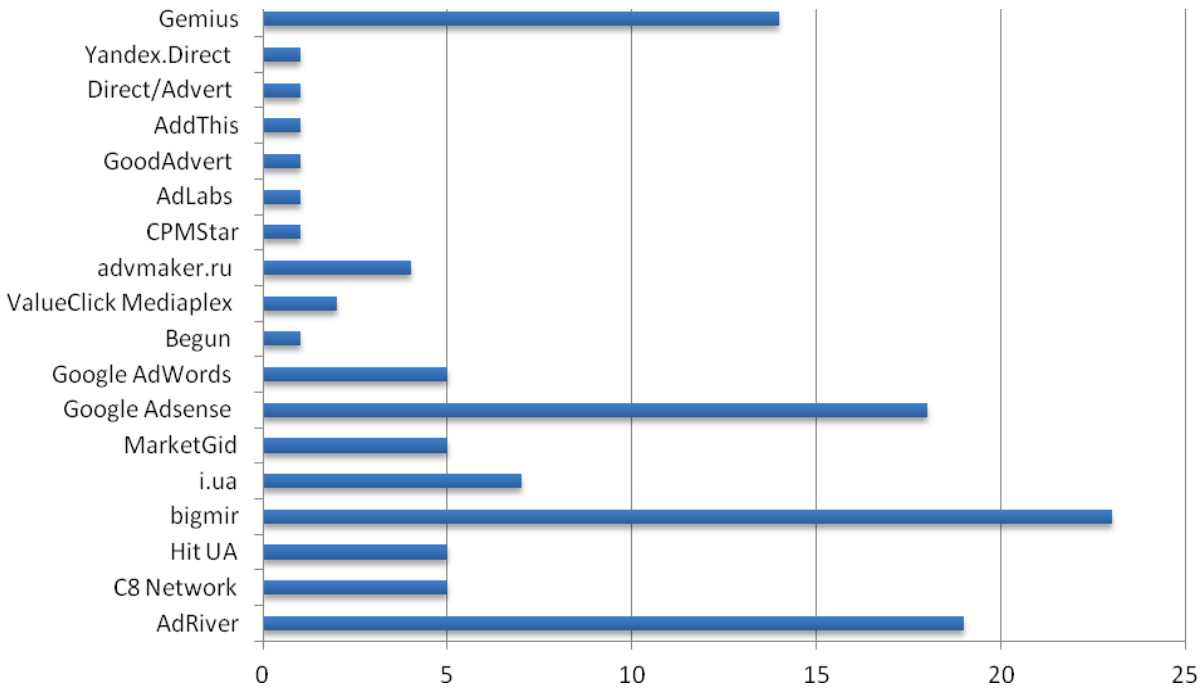

Рис. 5. Найпоширеніші технології web tracking типу Advertising

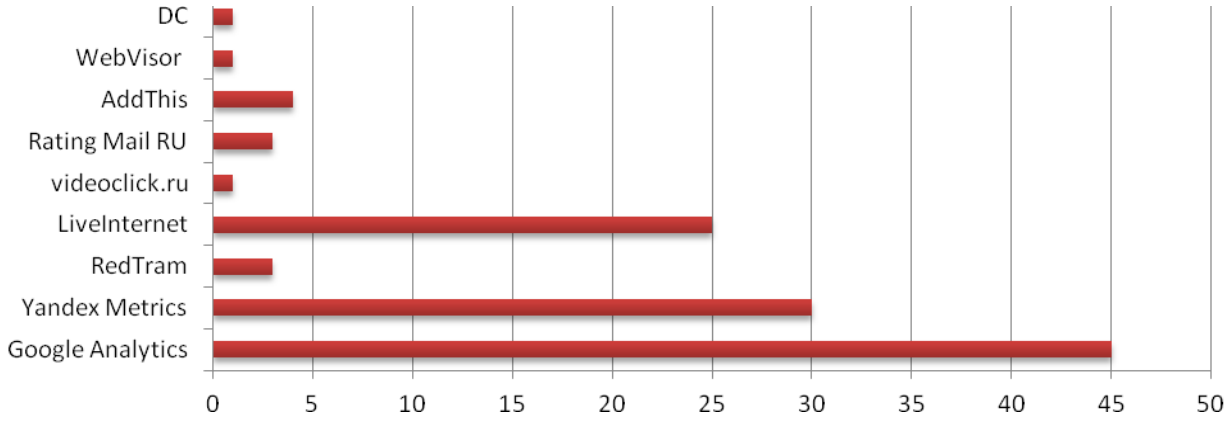

Рис. 6. Найпоширеніші технології web tracking типу Analytics

Процедуру авторизації на веб-ресурсі за допомогою соціальних мереж використовує лише 13% з вибірки веб-ресурсів. Усі 100% з вибірки веб-ресурсів використовують cookie, технологію ж flash LSO використовує 65% веб-ресурсів з категорії «Інтернет-медіа», в той момент, коли інші дві категорії їх практично не використовують.

Під час авторизації користувач дає згоду на передавання його персональних даних з його облікового запису у соціальній мережі до ресурсу, на якому він авторизується. Таким чином, соціальні мережі знімають з себе відповідальність за використання даних користувача третіми сторонами, що детально розписано в їх політиках конфіденційності.

При запиті на передавання даних користувача соціальні мережі чітко визначають склад даних, які будуть передані. Так, стандартний набір даних однієї з найпопулярніших мереж (facebook) має такий вигляд:

- унікальний ідентифікатор користувача у соціальній мережі,
- повне ім’я користувача,
- посилання на його обліковий запис,
- нікнейм,

– стать.

Без додаткової згоди користувача також є доступним його «аватар». Для отримання адреси електронної скриньки або доступу до альбомів користувача ресурс повинен здійснити запит на отримання додаткового дозволу.

Така інформація надсилається у форматі JSON (JavaScript Object Notation) (рис. 7) та може бути використана власником ресурсу для відображення на сторінці на свій розсуд і обмежена політикою конфіденційності.


```
{
  "id": "1214073125",
  "name": "Ivan Tiwari",
  "first_name": " Ivan ",
  "last_name": "Tiwari",
  "link": "https://www.socialnetwork.com/yogesh",
  "username": "yogesh",
  "gender": "male",
  "locale": "en_US"
}
```


Рис. 7. JSON формат персональних даних користувача

Соціальні мережі за окремою згодою користувача також надають можливість стороннім ресурсам публікувати матеріали від імені користувача, надають доступ до хроніки користувача або його адреси (залежно від політики конфіденційності конкретної соціальної мережі). Саме на оброблення цих даних може дати згоду користувач в процесі авторизації на веб-ресурсі.

Виявлено, що на деяких з вибірки веб-ресурсів присутні сторонні віджети авторизації у соціальних мережах (рис. 1), під час авторизації через які користувач дає згоду на передавання його даних не кінцевому веб-ресурсу, а сторонньому додатку, яких містить власну політику конфіденційності, можливо відмінну від цільового веб-ресурсу. Таким чином, під час авторизації користувач розкриває набір власних персональних даних не лише кінцевому ресурсу, а ще й ресурсу посереднику.

Наприклад, при реєстрації через такий сторонній додаток з використанням однієї з популярних соціальних мереж (twitter) користувач надає сторонньому додатку (Loginza) право на:

– читання повідомлень користувача,
– доступ до інформації про контакти.

Інший веб-ресурс при реєстрації через аналогічну соціальну мережу із застосуванням іншого стороннього додатку прагне отримати доступ до:

– повідомлень користувача,
– права рекомендації кола контактів,
– оновлення профілю користувача,
– публікацію повідомлень від імені користувача.

Через інші соціальні мережі ресурс здійснює запит на право доступу до фотоальбомів користувача, списку контактів, адреси електронної поштової скриньки. При об’єднанні декількох логінів користувача в одних обліковий запис виникає запитання про достатність (а точніше не надлишковість) об’єму даних, які збираються для забезпечення нормальної функціональності ресурсу.

Крім сторонніх додатків, що забезпечують авторизацію через облікові записи соціальних мереж, деякі з досліджених сайтів містять віджет (рис. 8), що забезпечує можливість коментування на веб-ресурсі. При цьому користувач змушений окремо проходити авторизацію в цьому додатку та надавати йому дані особистого профілю, адресу електронної пошти, право читання публічних повідомлень користувача, право на рекомендацію кола контактів, оновлювати обліковий запис та публікувати повідомлення від імені користувача, залежно від налаштувань соціальної мережі. Слід зазначити, що коментарі користувача зберігаються на стороні цього додатку.

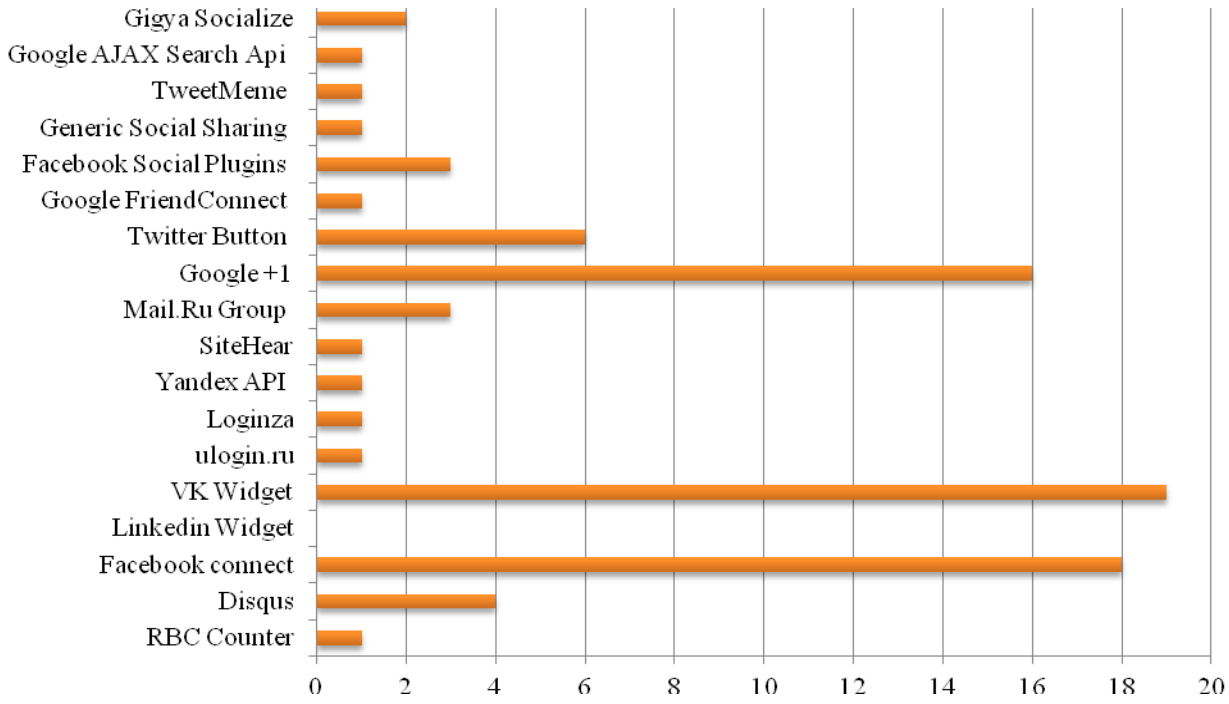

Рис. 8. Найпоширеніші технології web tracking типу Widgets

Крім цього досліджено склад та зміст flash cookie, які встановлюються на стороні користувача під час відвідування вибірки веб-ресурсів. Дослідження проводилось за допомогою додатку Minerva, який дає змогу переглядати та змінювати значення вже встановлених пар ключ значення.

Виявлено, що flash cookie встановлюються у 87% з вибірки веб-ресурсів (з них 65% при відвідуванні веб-ресурсів з категорії «Інтернет-медіа» (рис. 9).

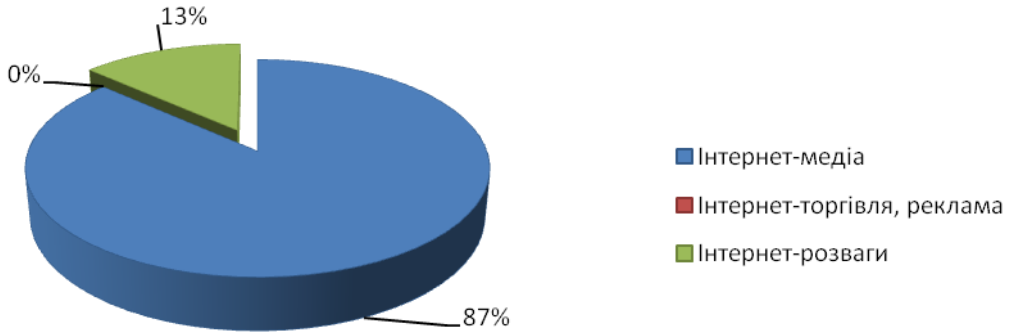

Рис. 9. Факт встановлення flash cookie при відвідуванні вибірки веб-ресурсів

Досліджуючи flash cookie при відвідуванні вибірки веб-ресурсів було записано унікальний ідентифікатор користувача, яким може бути використаний в процесі ідентифікації запиту та встановлення особи користувача.

Flash cookie зазвичай містять таку інформацію:

- дату встановлення,
- теперішню дату у форматі Unix timestamp,
- domain hash,
- expiration date,
- дату першого відвідування,
- дату останнього відвідування,

– кількість сесій (насправді кількість переходів між сторінками),
– унікальний ідентифікатор сесій,
– посилання-реферал, яке зазвичай вказує останній відвіданий веб-ресурс та останню відвідану на ньому сторінку,
– кількість звернень до стороннього ресурсу (код якого власне і встановив даний файл flash cookie).

Типовий ідентифікатор встановленого файлу flash cookie має таке значення:

Ключ	Значення
Uid	5DA267R9D1A71862357489SJ47R29V4A
sessionId	134574237945132000

Підсумувавши вищезазначене можна стверджувати, що внаслідок застосування розробниками та власниками веб-ресурсів сторонніх додатків для надання додаткової функціональності, інколи повноцінне використання веб-ресурсу можливе лише за умови надання власних персональних даних не лише власникам ресурсу, а й третім сторонам. Це стосується розкриття персональних даних користувача за його згодою через соціальні мережі.

Це відбувається під час авторизації через сторонні сервіси, коментуванні контенту веб-ресурсу за допомогою сторонніх сервісів. Після реєстрації через соціальні мережі веб-ресурс отримує основну інформацію про користувача, яка використовується для відображення облікового запису користувача. Саме цим можуть скористатися сторонні трекери. При наступному запиті крім унікального ідентифікатора користувача та службової інформації вони можуть включити до запиту на свої сервери ідентифікатор користувача у соціальній мережі, забезпечивши деанонімізацію користувача при надходженні наступних запитів.

Рекомендації щодо забезпечення приватності персональних даних в мережі Інтернет

Серед найдієвіших засобів мінімізації випадків відстеження діяльності та ідентифікації користувача є:

– застосування додатків до браузера, які здатні блокувати виконання скриптів та завантаження контенту трекерів,
– блокування виконання браузером javascript коду,
– відключення можливості встановлення веб-ресурсами flash cookie,
– відключення використання DOM Storage,
– відключення можливості встановлення cookie,
– контроль за кількістю та складом наданої персональної інформації веб-ресурсам.

Одним з найважливіших та першочергових кроків є обмеження виконання javascript функцій на веб-сторінці. Це не лише позбавить від нав’язливої реклами, але й вбереже від випадків атак фішингу з накладанням даних користувача на фон соціальної мережі, зменшить кількість запитів до ресурсів-трекерів, кожен з яких потенційно може містити персональні дані користувача або унікальний ідентифікатор, який здатен пов’язати користувача з цими даними. Заборонити виконання javascript файлів можна за допомогою додатку NoScript до браузера Mozilla Firefox. За його допомогою можна гнучко налаштувати політики безпеки для окремих веб-ресурсів, дозволивши виконання усіх скриптів на сторінці тимчасово або на постійній основі. Також за його допомогою можна блокувати лише скрипти, які надані третіми сторонами, дозволяючи виконання корисних скриптів на веб-ресурсі.

Більшість існуючих та функціонуючих на даний момент веб-ресурсів активно застосовують на своїх сторінках javascript для забезпечення валідації вводу користувача, надсилання асинхронних запитів на сервер, верстки сторінки та побудови динамічного контенту. Практично це означає, що javascript необхідний переважній більшості сучасних веб-ресурсів для забезпечення їх нормального та повного режиму функціонування. З іншої сторони це зумовлює web tracking через вбудовані третіми сторонами вставки коду.

Дієвим способом захисту персональних даних є використання додатків, що класифікують сторонні скрипти та блокують небажані. Серед таких додатків можна назвати додаток Ghostery до

Mozilla Firefox містить базу найпоширеніших трекерів, віджетів, ресурсів аналітики та реклами і має змогу блокувати їх відображення на сторінці та встановлення ними файлів coockie. Використання цього додатку дає змогу без блокування javascript обмежити встановлення файлів coockie та flash cookie сторонніми ресурсами. Але використання його одного не вбереже повністю, тому слід поєднувати з блокуванням javascript функції.

Варто відключити можливість встановлення flash cookie в налаштування adobe flash [15].

Також слід відключити збереження DOM storage. В браузері Mozilla Firefox це можна зробити перейшовши за посиланням about:config та встановивши значення властивості dom.storage.enabled у значення false.

Слід зазначити, що виконання одного або декількох з наведених вище кроків може вплинути на роботу веб-сторінки та обмежити її функціональність.

Ще одним яскравим прикладом збору персональних даних користувача є збереження історії пошуку компанією Google. Згідно політики конфіденційності це робиться з метою забезпечення кращої релевантності відображених результатів пошуку користувача.

Відключити збереження історії та видалити усі записи пошуку можна за посиланням [16].

Пошукова система від даної компанії тісно пов'язана з поштовим сервісом та широким спектром послуг, що надаються нею. З огляду на те, що ці послуги потенційно покривають більшість аспектів як професійної діяльності так і діяльності, направленої на розваги, зібрані таким чином дані потенційно можуть повною мірою відображати діяльність та інтереси користувача у мережі Інтернет.

В політиці конфіденційності вказано, що компанія зберігає інформацію про діяльність користувача, включаючи відвідані користувачем сторінки, історію та результати пошуку, включаючи персональні дані.

Згідно політики конфіденційності дана діяльність направлена на покращення взаємодії між користувачем та послугами та забезпечує кращу якість функціонування продуктів.

Крім зазначених кроків на відключення збереження результатів пошуку користувача можна використовувати сторонні пошукові системи які позиціонують себе як безпечні та як такі, що не відстежують роботу користувача. Однією з них є https://duckduckgo.com/.

Висновки

В роботі досліджено факти використання технології web tracking користувачів вибірки веб-ресурсів України. Для цього було визначено перелік сторонніх веб-ресурсів, що вбудовують свій функціонал в розмітку кінцевої сторінки. В межах дослідження було виявлено факти встановлення сторонніми веб-ресурсами своїх cookie та flash cookie файлів. Проаналізувавши ці файли, було виявлено факти встановлення унікальних ідентифікаторів з ключем, що впізнається як унікальний ідентифікатор користувача. Також було виявлено, що сторонні веб-ресурси підраховують кількість відвідуваних сторінок користувачем та визначають, які саме сторінки були відвідані.

Також було досліджено дані, право доступу до яких запитують ресурси при авторизації. Виявлено факти використання сторонніх додатків для забезпечення реєстрації та авторизації на кінцевому веб-ресурсі за допомогою облікових записів соціальних мереж. При цьому в деяких випадках сторонній додаток від соціальної мережі отримує дані з облікового запису користувача.

На основі отриманих даних обґрунтовано рекомендації користувачам щодо підвищення рівня забезпечення недоторканості їх приватного життя при використанні веб-ресурсів, шляхом встановлення обмежень на виконання сторонніх javascript функцій, блокування роботи сторонніх ресурсів, які віднесені до однієї з потенційно небезпечних категорій та унеможливлення встановлення файлів cookie браузером при переході користувача на веб-сторінку.

Список використаних джерел

1. *ARTICLE 29 DATA PROTECTION WORKING PARTY. WP 194. Opinion 04/2012 on Cookie Consent Exemption. Adopted on 7 June 2012 [Електронний ресурс] режим доступу: http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/files/2012/ wp194_en.pdf* ***2.*** *G.W. van Blarkom. Handbook of Privacy and Privacy-Enhancing Technologies – The case of Intelligent Software Agents / G. W. van Blarkom, J. J. Borking, J. G. E. Olk, J. Huizenga. – The Hague, 2003. – 352 p.* ***3.*** *Презентация проекта Декларации за обеспечение неприкосновенности частной жизни в Интернет [Електронний ресурс] режим доступу:* http://press.liga.net/releases/

prezentatsiya_proekta_deklaratsii_za_obespechenie_neprikosnovennosti_chastnoy_zhizni_v_internet/
4. *Декларація «За забезпечення недоторканості приватного життя в інтернеті» [Електронний ресурс] режим доступу: http://uapdp.org/images/1016%202012%20.pdf* ***5.*** *«Київстар» підтримує принципи Декларації «За забезпечення недоторканості приватного життя в Інтернеті» [Електронний ресурс] режим доступу: http://www.kyivstar.ua/press_center_new/news/?id=29624* ***6.*** *МТС приєдналася до декларації за забезпечення недоторканності приватного життя в інтернеті [Електронний ресурс] режим доступу:* http://company.mts.com.ua/ukr/press_releases.php*?news _id=6101* ***7.*** *Третій український форум з управління інтернетом [Електронний ресурс] режим доступу: http://igf-ua.org/docs/Resolution_IGF-UA_2012.pdf* ***8.*** *Рекомендація № R (99) 5 Щодо захисту недоторканності приватного життя в інтернеті [Електронний ресурс] режим доступу: http://www.medialaw.kiev.ua/laws/laws_international/105/* ***9.*** *Проведено перший громадський моніторинг інтернет ресурсів [Електронний ресурс] режим доступу: http://uapdp.org/index.php/podiji/khronika-podij/144-pershiy-monitoring* ***10.*** *Звіт №1 за результатами громадського моніторингу (лютий 2013) «Забезпечення прозорості та відкритості обробки персональних даних на веб-ресурсах» [Електронний ресурс] режим доступу: http://uapdp.org/images/news/doslidzhennya/Research-results-v.2.2.pdf* ***11.*** *Додаток А до Звіту №1 [Електронний ресурс] режим доступу: http://uapdp.org/images/news/doslidzhennya/Check-list-v.0.4.pdf* ***12.*** *Cookies [Електронний ресурс] режим доступу: http://www.compress.ru/article.aspx?id=16098&iid=736* ***13.*** *OWASP TOP 10 [Електронний ресурс] режим доступу: https://www.owasp.org/index.php/Top_10_2013-T10* ***14.*** *[Електронний ресурс] режим доступу: http://www.ghostery.com/* ***15.*** *[Електронний ресурс] режим доступу: http://www.macromedia.com/support/documentation/en/flashplayer/help/settings_manager03.html* ***16.*** *[Електронний ресурс] режим доступу: https://history.google.com/history/settings?hl=ru.*