УДК 002.6:681.142.37(004.2)

Гуцалюк Михайло Васильович –
кандидат юридичних наук, доцент, старший науковий співробітник

Впровадження ID-web як необхідна умова безпеки в Інтернет

У статті розглянуті питання ідентифікації користувачів у мережі Інтернет і запропоновано впровадження ID-web технології як необхідної умови безпеки в Інтернет.

Кількість користувачів Інтернет в Україні постійно зростає і на початок 2008 року становила близько 7,7 мільйонів, що на 20 % перевищує показники 2007 року та відповідно на 83 % у порівнянні з січнем 2006 року [1]. Слід зазначити що крім традиційних послуг, таких як розваги та перегляд новин, все частіше Інтернет використовується для переказу грошей, замовлення квитків, купівлі товарів в Інтернет-магазинах. Адже ці послуги, на відміну від стандартних у традиційних установах, здійснюються цілодобово з домівки чи офісу "не відходячи від комп'ютера" й за лічені хвилини можливо переглянути товар у декількох постачальників та вибрати оптимальні розцінки. Цікаво, що більш активному використанню системи електронних переказів цього року сприяли черги в установах Ощадбанку, які виникли в зв'язку з отриманням громадянами України компенсацій за вкладами СРСР.

Водночас, із поширенням використання Інтернет технологій, пропорційно зростає й загроза правопорушень, метою яких є хакерські атаки, викрадення персональної інформації, блокування роботи інформаційних служб, шантаж, шахрайство тощо [2]. Це обумовлено низкою причин, зокрема зростанням довіри до електронних засобів обробки інформації, розширенням кола суб'єктів – учасників інформаційних відносин у глобальній мережі, збільшенням кількості різноманітних сервісів, переходу до обслуговування банківських установ. Широкого розповсюдження в Інтернет сьогодні отримали різноманітні схеми, спрямовані на отримання коштів з недосвідчених та довірливих користувачів Інтернет-магазинів, віртуальних аукціонів, сайтів знайомств тощо. Зазвичай для такого виду шахрайства використовуються Інтернет-сайти, що візуально та за назвою нагадують відомі міжнародні ресурси. Проте, на відміну від добре зарекомендованих брендів, на отримання замовленого товару або повернення коштів годі й сподіватися. Причина користування такими ресурсами – бажання отримати замовлення за надзвичайно низькі ціни. Жадібність окремих громадян використовують і автори так званих "нігерійських листів", які пропонують за відповідний аванс надати певний відсоток коштів одного з африканських президентів або міністрів. Іноді зловмисники використовують і протилежні якості людини, наприклад, створюючи фіктивний сайт благодійного фонду або школи-інтернату.

Проблемам протидії правопорушенням у сфері використання Інтернет-технологій присвячено чимало праць як західних, так і вітчизняних науковців. Так, у роботах В. Бутузова, В. Гавловського, В. Голубєва, Р. Калюжного, Б. Романюка, В. Цимбалюка та інших фахівців наголошується на необхідності вдосконалення чинного законодавства, що регулює інформаційні відносини, зокрема розробки Інформаційного Кодексу, розбудови відповідних організаційних структур правоохоронних органів для виявлення та розслідування цих специфічних видів злочинів, професійної підготовки спеціалістів для цих підрозділів тощо. Основні

засади вищеназваних пропозицій викладено у Концепції реформування законодавства України у сфері суспільних інформаційних відносин та у Концепції стратегії реалізації державної політики щодо боротьби з кіберзлочинністю в Україні, які розміщені на сайті Міжвідомчого науково-дослідного центру з проблем боротьби з організованою злочинністю [3].

Наголошується також на тому, що основні складові проблеми виявлення та розслідування правопорушень в Інтернет полягають у відсутності державних кордонів у глобальній мережі та складності, а часом повної неможливості ідентифікації користувачів (юзерів – англ. user) інформаційних ресурсів. Саме можливість працювати в Інтернет анонімно, не надаючи відповідної інформації про себе в надії про повну безкарність, і спонукає зловмисників на нові правопорушення. Адже, на сайті дуже просто розмістити фотографію відомої особи та видавати себе за неї. Скажімо на сайті "однокласники" після створення сторінки Ю. Тимошенко відразу з'являється багато бажаючих поспілкуватися з "нею". А за повідомленням представників управління "К" Російської Федерації громадянину Німеччини, який був схвильований відсутністю "нареченої", з якою той познайомився через Інтернет та надіслав 26 тис. євро, у Москві пояснили, що на фото зображена відома російська балерина Анастасія Волочкова. Такі сайти знайомств адмініструються декількома програмістами, перекладачами та контролюються кримінальними авторитетами. Ще більш складну організаційну структуру утворюють інформаційні мережі, створені для розповсюдження дитячої порнографії. В них задіяні правопорушники не тільки з різних міст, але й з різних держав. У певних містах однієї країни створюються спеціалізовані студії, з серверів другої держави відбувається трансляція, а фінансові потоки акумулюються в третій. Розслідування таких злочинів потребує не тільки відповідної технічної підготовки, але й тісної міжнародної координації правоохоронних органів. Для цього країни великої вісімки створили цілодобові контактні пункти для координації дій щодо протидії комп'ютерній злочинності та електронним доказам тяжких злочинів.

Однією з найперших вдалих операцій щодо протидії поширення дитячої порнографії була операція, проведена у 2003 році правоохоронцями США, Канади, Німеччини, Норвегії та Великобританії, тоді були заарештовані адміністратори 17 сайтів, які знаходилися в 7 різних країнах світу. Під час операції "Коала" у 2007 році, що проходила за координацією Європолу було заарештовано 92 особи. В операції були задіяні поліцейські з вісімнадцяти європейських держав та Австралії.

На жаль, хоча значна кількість "продукції" постачалася з України, в МВС України до цього часу не створені відповідні організаційні структури. Це, зокрема, призводить до того, що електронною поштою відкрито пропонують послуги щодо розсилки спаму або порнографічної продукції, що схоже на відкриту рекламну акцію тестування наркотиків на Хрещатику, проте, незважаючи на відповідну статтю Кримінального Кодексу України, реакція правоохоронців відсутня. Для прикладу, в США за розповсюдження спаму житель міста Райлі Джеремі Джейнс (штат Вірджинія) був засуджений до 9 років позбавлення волі. Подібні кримінальна відповідальність передбачена в усіх штатах, а також у державах Європи та інших країнах світу. Відсутність покарання за подібні правопорушення в Україні призводить до того, що наша держава стає своєрідною Меккою для спамерів.

Традиційно для ідентифікації користувача в інформаційних системах використовують дві складові – логін та пароль, при цьому сам користувач залишається анонімним (він відомий тільки за своїм логіном). При користуванні різноманітними інформаційними системами потрібно використовувати нові "свої" логіни, адже використаний раніше логін може вже зайняти інший користувач. Згодом у конкретної фізичної особи їх може налічуватися декілька десятків. У той

же час, наприклад, при користуванні чатом (програмою обміну відгуками про подію – обговоренням) ваш логін може захопити інший користувач.

У 2008 році для об'єднання зусиль, спрямованих на спрощення процедури реєстрації користувачів на Web-сайтах провідні світові компанії, пов'язані з інформаційними технологіями, такі як IBM, Google, Microsoft, VeriSign і Yahoo увійшли до складу асоціації OpenID Foundation. Інфраструктура OpenID дозволить користувачам використовувати єдиний логін і пароль для реєстрації на будь-якому сайті, що підтримує дану технологію. На сьогодні налічується вже понад 10 тис. користувачів, які використовують технологію OpenID.

Іншим важливим елементом для ідентифікації особи може слугувати унікальна IP- адреса користувача, яка на думку західних науковців повинна розглядатися як персональні дані. Зокрема, в Ізраїлі наприкінці 2007 року були прийняті відповідні законодавчі поправки з метою отримання правоохоронними органами таких даних для прискорення розшуку правопорушників.

Проте, цей, на перший погляд, ідеальний варіант ідентифікації має декілька недоліків. По-перше існують відповідні веб-сайти, що можуть змінювати IP- адресу користувача. По-друге, якщо користувач має доступ до провайдера не безпосередньо, а через внутрішню мережу, наприклад певної установи, кількість комп'ютерів у якій може становити сотні і тисячі, то ідентифікувати особу стає вкрай важко. Але найголовнішим є те, що, наприклад, з вашого комп'ютера доступ до глобальної мережі може отримати зовсім інша особа, скажімо ваш співробітник, технічний працівник, або взагалі сторонній суб'єкт.

Вирішення питання щодо ідентифікації особи в Інтернет можливе завдяки використанню біометрії людини. Цей спосіб у новому тисячолітті досить широко використовують для захисту ідентифікаційних документів, отримання доступу як до технічних пристроїв, так і приміщень чи інших об'єктів тощо [4].

На нашу думку, для ідентифікації користувачів Інтернет слід використовувати наступний механізм з умовною назвою "ID-web технології" (ідентифікація веб-користувачів). Певні біометричні дані, що повинні бути визначені відповідними нормативно-правовими документами, наприклад відбитки пальців, можна використовувати як цифровий підпис особи, механізм використання якого вже законодавчо визначений [5]. На відміну від традиційного електронного цифрового підпису, яким може скористатися стороння особа, "біометричний" підпис надає можливість провести аутентифікацію особи безпосередньо за її робочим місцем. Причому можуть використовуватися й безконтактні методи аутентифікації, наприклад з використанням 3D біометрії (використовується опис обличчя фізичної особи), голосу або в комплексі декілька біометричних характеристик особи. Інформація про біометричні характеристики особи повинна зберігатися у відповідних банках даних із специфічним механізмом доступу до нього та комплексною системою захисту інформації.

Роботи щодо створення подібних банків даних ведуться в різних країнах. Зокрема, заступник голови Європейської комісії, комісар з питань юстиції, свободи та безпеки Франко Фраттіні повідомив, що Європейський союз (ЄС) планує ввести процедуру зняття відбитків пальців гостей (на в'їзді і виїзді) всіх 27 країн блоку. Але найбільшим, мабуть, проектом щодо збереження біометричних даних є відповідний Банк даних ФБР, на модернізацію якого в найближчі роки уряд США виділив понад 1 млрд доларів [6].

В Україні збір біометричної інформації законодавчо досі не визначений. Можливо це пов'язано з очікуванням відповідних стандартів Європейського Союзу, які планується затвердити вже в 2008 році. Проте, сама ідея опрацювання такої інформації вже активно обговорюється науковцями та практиками. Скажімо, вже сьогодні йде розробка автоматизованої інформаційно-аналітичної системи органів

законодавчої діяльності “Рада-4”, в якій для ідентифікації народних депутатів, з метою унеможливлення голосування за відсутніх колег, будуть використовуватися їх біометричні дані [7]. А Кабінет Міністрів України Постановою від 12 березня 2008 р. № 439-р зобов’язав низку міністерств “провести аналіз стану використання та розвитку біометричних технологій в правоохоронній та інших сферах, наявності на внутрішньому ринку вітчизняних програмних і технічних засобів оброблення біометричних даних, за результатами якого підготувати із залученням фахівців установ та організацій – постачальників аналогічної техніки, і науковців проектно-технічні рішення стосовно впровадження біометричних технологій в інтегрованій міжвідомчій інформаційно-телекомунікаційній системі щодо контролю осіб, транспортних засобів та вантажів, які перетинають державний кордон” [8].

Але постає питання, чи згодні будуть користувачі мережі Інтернет, яка з самого початку передбачала анонімність. Я вважаю, що тут повинен діяти принцип добровільності. Якщо ти бажаєш працювати анонімно – працюй. Проте, інші користувачі, а особливо в електронній комерції, все ж-таки віддадуть перевагу достовірній ідентифікації чи то клієнта, чи то власників web-ресурсу.

Список використаних джерел

1. *Журнал* Компаньон online [Електронний ресурс] / <http://www.companion.ua>.
2. *Виявлення* та розслідування злочинів, що вчиняються у сфері інформаційних технологій: Наук. – практ. Посіб. / Б.В. Романюк, В.Д. Гавловський, М.В. Гуцалюк, В.М. Бутузов. – К.: Вид. ПАЛИВОДА А.В., 2004. – 144 с.
3. *Міжвідомчий* науково-дослідний центр з проблем боротьби з організованою злочинністю при Раді нац. безпеки і оборони України [Електронний ресурс] / <http//:mndc.naiau.kiev.ua>.
4. *М. Гуцалюк* Ідентифікація фізичних осіб // Право України. – 2006. – № 5. – С. 122 – 126.
5. *Закон* України від 22 травня 2003 року № 852-IV “Про електронний цифровий підпис” // Відомості Верховної ради України. – 2003. – № 36. – Ст. 276.
6. *ЄС хоче* знімати відбитки пальців у своїх гостей // Газета по-українські [Електронний ресурс] / <http://www.gpu.ua>, 21 січня 2008 р.
7. *Нова* “Рада” обійдеться в сім мільйонів // Львівська газета. – № 38, – 18 березня 2008 р.
8. *Розпорядження* Кабінету Міністрів України від 12 березня 2008 р. № 439-р. [Електронний ресурс] / <htth://liga.net/laws/>.

The article is dedicated to the questions of users` identification in the Internet. The author offers to introduce ID-web as a requirement of the Internet safety.