

ВІД РЕДАКЦІЙНОЇ КОЛЕГІЇ*неофіційний переклад***Заява Комітету Парламенту Канади з питань громадянства та імміграції
від 4 жовтня 2003 року****“НАЦІОНАЛЬНІ ІДЕНТИФІКАЦІЙНІ КАРТКИ (ПОСВІДЧЕННЯ ОСОБИ)”**

Ця письмова заява є наслідком зустрічі між Прайвесі Інтернешнл (Privacy International) і Комітетом Парламенту Канади з питань громадянства та імміграції (далі Комітет), що відбулася за зверненням Комітету 24 червня 2003 року у Лондоні (Велика Британія).

Прайвесі Інтернешнл переконливо рекомендує Комітету підходити до проблеми ідентифікаційних карток з великою пересторогою. Багато які з умов, що пред’являються для технології на основі карткової системи не можуть бути підтримані. Обґрунтування руху у напрямку до цієї картки може в окремих випадках робитися з добрими намірами, але здається, що воно засновується більше на емоціях і балаканині, аніж на вірогідному дослідженні.

Біометрична система, запропонована для формування ідентифікаційної бази для картки, не має успішного зразку будь-де у світі. Свідчення дослідників стверджують, що багато з заяв, зроблених біометричною промисловістю, є неправдивими. Насправді, архітектура біометрії, яку уявляють собі деякі прихильники канадської схеми, є повністю шахрайською.

Вартість системи ідентифікаційних карток, разом з відповідними реєстраційними процедурами, інфраструктурою технологій, узгодженням приватного і публічного секторів і рівнобіжних систем буде значно більшою від неофіційних оцінок, що поширюються на даний час. Базуючись на кошторисах Великої Британії, Європи і Південно-Східної Азії, ми оцінюємо, що канадська система, на момент повного завершення, коштуватиме 7 мільярдів канадських доларів.

Загроза приватності, що виникає в результаті впровадження національної ідентифікаційної системи, не може бути переоцінена. Ідентифікаційні картки в канадському (суспільному) оточенні, імовірніше за все, порушуватимуть Хартію прав і свобод. Картка істотно порушить приватність і принципи захисту даних, передбачені в канадському праві.

У дослідницькій літературі відсутні жодні докази для того, щоб встановити, що ідентифікаційні картки зменшують загрозу тероризму чи зменшують сферу злочинності. Насправді, впровадження ідентифікаційної картки потягне створення нової низки правопорушень і внесе цілком реальну загрозу зростання злочинності в значній кількості областей.

Ідентифікаційна картка, запропонована для Канади, передбачає концепцію зведених чи “об’єднаних” ресурсів даних. Такий стан створює серйозну загрозу безпеці даних. Видається неминучим, що дані будуть загублені, перекручені, видозмінені чи незаконно використані. Доступ великої кількості агенцій до даних значно підвищує імовірність неналежного використання інформації або через розкриття, спричинене корупцією, або через недоліки у безпеці.

Короткий огляд

Протягом минулих двадцяти років уряди багатьох країн впроваджували національні ідентифікаційні картки. Прихильники таких систем наводили усе більше і більше доказів на користь прийняття поєднання усесторонньої інформації про особу та біометричного ідентифікатора, на кшталт сканування райдувної оболонки чи відбитків пальців. Велика Британія і Канада, на даний час, розглядають такі системи, у той час як Бельгія і Китай знаходяться на перших стадіях впровадження ідентифікаційних карток.

Формулювання обґрунтування схем ідентифікації значно відрізняється, але звичайно стосується кількох усвідомлених переваг, зокрема, зменшення шахрайства, зростання адміністративної ефективності і боротьби з незаконною імміграцією.

Разом з тим часто наводиться зауваження, що карткова система може слугувати каналом “побудови нації”, завдяки чому можуть бути посилені єдність і національна ідентичність. Ці інтуїтивні зауваження не мають жодного відношення до формулювання обґрунтування карток. У цьому сенсі картка може виступати ініціативою, в основі якої лежить націоналізм.

Опікування ідеєю про ідентифікаційні картки здійснюється з невеликою кількістю доказів, що підлягають вимірюванню, стосовно вимог, які пред’являються до карткової системи. Припущення, наприклад, що національна картка може поліпшити методи правоохоронної діяльності, знизити рівень незаконної імміграції, зменшити шахрайство, допоможе національній безпеці чи покращить адміністративну ефективність, є суто інтуїтивним. Існує небагато, якщо вони взагалі є, доказів того, що карткова система може досягти цих цілей.

Основну причину такої ситуації слід шукати в типі націоналізму, згаданому раніше. Країни, на кшталт Малайзії, Китаю, Сінгапуру та Індонезії, відкрито сприяють цим карткам як засобу встановлення національного “членства” і єдності. Торік у Великій Британії ця позиція була виражена проурядовим парламентарієм, доктором Ніком Палмером, який сказав на публічній зустрічі, присвяченій ідентифікаційним карткам, що він відчуває, що ідентифікаційна картка може створити “зв’язок” поміж усього населення. Карткова система часто носить назву чи символ країни (як, наприклад, вже не чинна картка Австралії і картка Ківі).

Біометрична система, запропонована для канадської картки, є необґрунтованою в своїй основі. Китай недавно відмовився від розміщення відбитків пальців на своїх ідентифікаційних картках через нездоланні технічні проблеми [1], тоді як Британська фінансова група “Nationwide” цього року відмовилась від планів запровадити зняття відбитків пальців і сканування ока на заміну PIN-коду [2].

Американські експерти з безпеки Пітер Нойман і Лаурі Вейнстейн відзначали: *“Вважається, що унікальні ідентифікаційні картки часто підробляються. Діє велика кількість груп підробників ідентифікаційних карток, як для кримінальних, так і для терористичних цілей. До цього часу кожна спроба посилити захист посвідчень особи від підробки була скомпрометована. Крім того, зловживання з боку утаємниченої особи – особливий ризик будь-якої інфраструктури посвідчень особи”*.

“Віра в те, що національні ідентифікаційні смарт-картки можуть забезпечити незаперечну біометричну відповідність без некоректних підтверджень або заперечень, є помилковою. Крім того, такі системи усе ще будуть “проламуватися”, а злочинці і терористи, щодо яких ми найбільше стурбовані, знайдуть спосіб експлуатувати їх, використовуючи фальшиве відчуття безпеки таким чином, що картки забезпечуватимуть їхню власну перевагу – фактично ставлячи нас у меншу безпеку в результаті цього” [3].

Існують також істотні загрози безпеці, що виникають як результат системи ідентифікації, заснованої на біометричних характеристиках. Експерт з комп’ютерної безпеки Брюс Шнейер (Bruce Schneier) застерігає: *“Обробка біометричних характеристик також має свої недоліки. Уявіть собі, що Аліса використовує відбиток свого великого пальця для біометрії, а хтось вкраде цифровий файл. Що тепер? Це не цифрове посвідчення, коли певна довірена третя особа може видати їй інше. Це – її великий палець. Вона має їх тільки два. Як тільки хтось вкраде ваші біометричні характеристики, вони залишаться вкраденими на все життя; не існує жодного способу повернутися до безпечної ситуації”* [4].

Ця заява обговорює значення і ризики, пов’язані з національними ідентифікаційними картками, із спеціальним посиланням як на біометричну, так і на інформаційну відповідність. Цей документ оцінює аргументи, що просувають використання цієї технології, і вагу цих доказів з юридичної, соціальної і технічної перспективи.

Ключові питання і засади

Пропозиції щодо впровадження урядових систем ідентифікаційних карток викликають суперечності в усьому світі. Парламенти Великої Британії і Канади на даний час розглядають національні схеми, результатом яких була б комплексна обов’язкова система ідентифікації. Австралія, Нова Зеландія і Сполучені Штати також мудрують з цією ідеєю, але зустрічають жорст-

кий політичний опір. Країни, що розвиваються, нестримно поспішають запровадити системи ідентифікації, тоді як у всій Європі уряди досліджували можливість розширення функціонування ідентифікаційних карток. Усі такі ініціативи зустрілися з непередбаченими і надзвичайно складними юридичними, технічними та організаційними проблемами.

Такі заходи завжди породжували дебати щодо їхнього потенційного впливу на приватність і громадянські права. Незважаючи на те, що вони є вирішальними, наслідки технології набагато істотніше і стосуються куди ширшої сфери. В своїй сутності, ці системи незмінно прокладають шлях до приєднання до управління і розвитку комплексного зв'язку між публічним і приватним секторами інформаційних систем.

Більше ніж протягом двох десятиліть дискутувалась аргументація: громадянські свободи проти ідентифікаційних карток. Правозахисники послідовно доводили: мало того, що такі ініціативи перетворюють нації на більш авторитарні суспільства, але вони назавжди істотно змінять відносини між громадянином і державою, природу уряду і характер нації.

Цей глибокий вплив є неминучим, оскільки сучасні ідентифікаційні картки – не просто шматочок пластмаси. Це видима складова надзвичайно складної мережі інтерактивної технології, що об'єднує найбільш інтимні характеристики особи з державним механізмом. Це також засіб, через який, теоретично, може бути як спрощено, так і розширено юридичні і адміністративні повноваження уряду.

Майже кожна національна ідентифікаційна карткова система, впроваджена протягом останніх п'ятнадцяти років, містила три компоненти, які потенційно можуть зруйнувати свободу особи і приватність. Спочатку кожен громадянин може бути зобов'язаний здати відбитки пальців чи візерунок сітківки до національної бази даних. Ця інформація об'єднується з іншими персональними даними на кшталт раси, віку і місця проживання. Фотографія довершує досє. Тоді, для того, щоб надати картці необхідної юридичної ваги, її впровадження повинно супроводжуватися суттєвим зростанням поліцейських повноважень. Органи влади, зрештою, вимагатимуть картку в широкому колі випадків, і люди будуть змушені підкоритися. Найбільш істотною, а разом з тим найбільш тонкою складовою є той факт, що картка і її кодова система згодом формуватимуть адміністративну основу для пов'язування інформації між усіма відомствами. Код, врешті-решт, є найбільш потужним елементом системи.

Для такої системи, пов'язаної десятками тисяч пристроїв для читання карток з центральною базою даних, звичайною справою є проблема підроблених карток. Технологічний розрив між урядами й організованою злочинністю тепер звузився до такого ступеня, що бланки навіть найбільш захищених карток стають доступними через тиждень після їхнього офіційного представлення. Злочинці і терористи можуть насправді пересуватися більш вільно і більш безпечно з декількома підробленими індивідуальностями, ніж вони могли б це робити в країні із численними формами посвідчення особи.

Для того, щоб упевнитися, що люди є саме тими, за кого вони себе видають, картки нового покоління на кшталт представлених торік у Малайзії містять чіп з біометрією – відскановані відбитки пальців, рук чи візерунок сітківки – власника. Картка і палець поміщені в пристрій читання – і особу “підтверджено”. Органи влади мають доступ до детальнішої персональної інформації, що зберігається на чіпі, для того, щоб підтвердити особу власника. Цей процес підтвердження може бути застосований на вулиці, в аеропортах, школах, банках, басейнах чи приміщеннях офісів. Для того, щоб картки слугували меті боротьби з тероризмом і крадіжкою ідентичності, вони повинні б використовуватися як механізм підтвердження багато разів на день, у незчисленних випадках.

Цей тверезий висновок рідко наводиться урядом. Натомість, такі ініціативи м'яко замасковані під виглядом картки громадянина, які забезпечують право на соціальні послуги і допомогу і які спрощують ведення справ особи з урядом. П'ять років тому, після останніх дебатів у Великій Британії щодо ідентифікаційних карток, уряд спокійно поховав такі пропозиції, коли виявив, що картка коштуватиме на мільярди фунтів більше, ніж очікувалось, робить небагато для запобігання злочинам, і може, на завершення, стати надзвичайно непопулярною ініціативою [5].

В останніх двох випадках, коли концепція ідентифікаційної картки була серйозно поставлена у Великій Британії, стало зрозуміло, що підтримка ідентифікаційних карток, в кращому випадку, є неоднорідною. Востаннє щодо цього висловилося (злочин був проблемою, що обговорювалась) навіть Асоціація керівників поліції (Association of Chief Police Officers), яка стверджувала, що картка матиме невеликий вплив на злочинність і може зашкодити стосункам між поліцією і громадськістю.

Це правда, що часи і обставини змінюються, але якщо ідентифікаційна картка п'ять років тому була непрацездатною, чому вона працюватиме зараз? Коротка відповідь на це питання полягає в тому, що на той час вона не могла працювати, доки не було додано біометричні характеристики, і вся система не отримала змогу діставати підтвердження через національну базу даних. Тоді, це – не картка: це – національна інфраструктура спостереження.

Посвідчення особи можуть також робити свій внесок у зростання рівня тероризму і злочинності. Торік у Нью-Джерсі було обвинувачено 36 осіб за їхню участь в злочинній організації, що випускала тисячі підроблених ліцензій водіїв. Також було заарештовано вісім осіб з персоналу Відділу транспортних засобів Нью-Джерсі.

Для країни, у якій ліцензія водія є найближчим відповідником до ідентифікаційної картки (національні картки завжди були неприйнятні для Конгресу), арешти викликали досить широке занепокоєння. Речник Відділу кримінальної юстиції Нью-Джерсі сказав “Нью-Йорк Таймс”, що місця для стоянки автомобілів Відділу транспортних засобів, принаймні у шістьох округах, були подібні на “барахолку незаконних документів”. Особи з персоналу підрозділу у окрузі Вейн отримали від 50 до 100 доларів за кожен з приблизно 3000 ліцензій.

Корупція зсередини – це кара для уряду, яку не наслідують називати. Тепер, незважаючи на свій намір підсилити захист ліцензій водіїв, США зневірилися у чесності своїх первинних засобів ідентифікації. Корупція в подібному масштабі оточує більшість офіційних схем ідентифікаційних карток. Високий попит і величезні інвестиції злочинців спокушають посадових осіб обходити чи порушувати правила прийнятності. Те ж саме є неминучим у Канаді та інших країнах.

Досвід у Нью-Джерсі – один з багатьох факторів, що повинні стримати щенячий ентузіазм будь-якого уряду щодо потенційних переваг ідентифікаційної карти. Міністри уявляють інструмент, який приборкає незаконну імміграцію, усуне злочини і шахрайство, зменшить ухиляння від податків і перешкодить тероризму. У дійсності, вони розпочали проект, що може значно посилити і ускладнити ці проблеми.

Розглянемо практичну сторону. Яким чином пересічний громадянин йтиме до одержання ідентифікаційної картки? І яким чином це відрізнятиметься від способу, яким злочинець, терорист чи незаконний іммігрант одержуватиме її?

Протягом років західні уряди, в усіх своїх консультаціях з цього центрального пункту, грали у мовчанку. Будь-яка ідентифікаційна картка, імовірно, видаватиметься особі на персональному інтерв'ю, можливо, подібному до процесу одержання Номера Соціального Страхування чи ліцензії водія Нью-Джерсі. Претендент може прийти на зустріч з нижчою посадовою особою, яка механічно запитає щодо двох форм ідентифікаційної картки і доказу місця проживання. Претенденту задали б кілька стандартних питань, після чого ідентифікаційна картка може бути формально видана.

Якщо перед цим вони могли принести копію свідоцтва про народження мертвої людини, і, можливо, ліцензію водія і номер рахунку в банку, тепер злочинці володітимуть основною ідентифікаційною картою, яка не задає жодних питань. Можливо, навіть більше, ніж однією такою ідентифікаційною картою.

Ідентифікаційна картка, зрештою, є тільки збільшенням високої цінності первинних документів особи, представлених її власником. Адміністрація США мала можливість пересвідчитися, що саме тут міститься фундаментальний недолік у понятті безпомилкової ідентифікаційної картки.

Після нападу на США 11 вересня ФБР оголосило, що принаймні четверо з повітряних піратів одержали чинні ліцензії водіїв США. Для Відділу транспортних засобів Вірджинії, приче-

тність якого до цього було виявлено, це був один з найсерйозніших моментів протверезіння у його тривалій історії. Органи влади Вірджинії розпочали шалену перевірку своїх процедур подання заявок, але повідомили, що існує досить мало можливостей запобігти цій проблемі.

Точно так само як усі, хто видає такі картки в усьому світі, відділ ліцензування не мав жодного вибору, крім того як покладатися на стандартні документи щодо особи, дійсність яких важко визначити. Як тільки претендент отримав НСС, паспорт, свідоцтво про народження і, можливо, рахунок в банку, усі критерії для видання ліцензії буде виконано. Що ще може зробити орган влади, щоб встановити право на ліцензію?

Одна проблема для вірджинських органів ліцензування, якої неможливо уникнути, полягала в тому, що в реальному світі одна основна форма посвідчення особи використовується для того, щоб отримати іншу форму посвідчення особи. Дві форми посвідчення особи ведуть до надання третьої. І так далі. У вільному суспільстві існує межа щодо ступеня, до якого уряд може поставити вимогу особи щодо розкриття цих документів.

Все ж таки органи ліцензування Вірджинії “накрутили хвоста” своєму персоналу, застерігаючи їх бути особливо допитливими при роботі із заявами. *“Не драгуйте наших клієнтів, – порадило вище керівництво, – але зробіть усе, що ви можете, щоб встановити потенційних терористів і незаконних мігрантів”*. За винятком деяких незначних змін, процедура авторизації зберігається як і раніше, з тією відмінністю від попередньої, що, безсумнівно, фальсифікація посвідчень особи коштуватиме дорожче.

А якщо заявники не мають необхідних документів? Який це подарунок у пошуку зайвих грошей для корумпованих державних службовців чи персоналу за контрактом! Корупція серед чинів державних службовців є фактом життя. Після двохлітнього слідства Незалежна Комісія Нового Південного Уельсу проти корупції в Австралії засвідчила у 1992 році, що корупція в державній службі досягла “пропорцій епідемії і ендемії”.

Ще більше погіршить перспективу схеми ідентифікаційних карток сценарій, за яким до вирішення цієї проблеми буде залучено приватну компанію, або, навіть ще гірше, її буде “скинуто” на вже перевантажену урядову агенцію.

Уряди можуть дозволити собі ігнорувати загрозу корупції серед чинів організації, що розглядається, однак банки не настільки наївні. Вони застосовують «модель загрози», що передбачає рівень корупції персоналу від одного до двох відсотків.

Навіть без перспективи офіційної корупції технологічний розрив між урядами й організованою злочинністю тепер звужився до такого ступеня, що навіть бланки найбільш захищених карток доступні через кілька тижнів після їхнього представлення. Злочинці і терористи можуть, насправді, рухатися вільніше і безпечніше з декількома підробленими “офіційними” індивідуальностями, ніж будь-коли в країні, використовуючи багаторазові форми посвідчень «низької вартості», на кшталт свідоцтва про народження.

Злочинне використання підроблених ідентифікаційних документів не обов'язково включає використання методів підробки. У 1999 році у Великій Британії колишній державний контролер був обвинувачений в одержанні до 500 паспортів на фальшивих осіб. Шахрайство було просто результатом маніпулювання під час процедури первинного документування.

Доцільно розглянути деякі неминучі формули, що застосовуються всупереч правилам економіки чорного ринку. Кожен раз, коли уряди намагаються запровадити ідентифікаційну картку, в основі завжди лежить мета усунення фальшивої індивідуальності. Чим вище “цілісність” (надійність і точність) картки, тим більшою є її цінність для злочинців і незаконних іммігрантів. Картка, що має високу цінність, притягує значно більші інвестиції у корупцію та підробку. Рівняння просте: вища цінність посвідчення особи дорівнює інтенсивнішій злочинній діяльності.

Коли такі схеми впроваджуються в поточній суспільній атмосфері, неминучими є три результати. Перший: високо захищена ідентифікаційна картка стане внутрішнім паспортом, необхідним в безлічі ситуацій. Не виходьте зі свого дому без неї. Другий: мільйони людей будуть страждати від серйозних незручностей щороку, через загублені, вкрадені чи пошкоджені картки або – через ще більш потенційно руйнівну причину – через відмову карткових комп'ютерних систем чи біометричних машин зчитування. Нарешті, як свідчить дослідження Прайвесі Інтер-

нешнл, картки будуть неминуче використані для зловживання з боку посадових осіб, які використовуватимуть їх як механізм для упередження, дискримінації чи переслідування. Цей останній пункт був сформульований Високим Судом Великої Британії у 1954 році, коли він визнав незаконними ідентифікаційні картки воєнного часу.

Інші країни також дійшли такого висновку. Жодна країна загального права не запроваджувала ідентифікаційних карток. Коли у 1986 році в Австралії було запропоновано національну картку, ця ідея була квапливо переглянута після найбільшої у сучасній історії суспільної опозиційної кампанії. Громадськість Нової Зеландії відповіла з подібною енергією, тоді як Сполучені Штати традиційно виступають проти національних карток.

Їхні побоювання добре обґрунтовані. Зокрема, за минулі вісімнадцять місяців національні лідери в обох півкулях з дивним смакуванням стверджували, що прагнення до більш безпечного суспільства повинно спонукати до переоцінки особистих свобод і приватності. Іншими словами, йдеться про встановлення істотного розширення повноважень держави щодо здійснення контролю за всіма громадянами і зміщення балансу на користь всебічного спостереження за населенням. Саме ідентифікаційна картка стала найбільш виразним проявом цього прагнення до більшого спостереження.

Ще однією підставою є її вартість. П'ять років тому уряд Великої Британії оцінив, що повна вартість виробництва і управління картою становитиме 20 фунтів стерлінгів на особу. Базова вартість біометричної картки в наші дні вимагатиме щонайменше 45 фунтів. В цілому витрати становлять більше двох мільярдів фунтів стерлінгів. Це число потроїться, коли ми врахуємо вартість модифікації комп'ютерної системи, реєстрацію біографічних даних і узгодження з приватним сектором. Уповноважений з питань приватності Канади нещодавно оцінив, що вартість національної картки в його країні становитиме близько п'яти мільярдів канадських доларів. Базуючись на даних Великої Британії і Європи, Прайвесі Інтернешнл оцінює вартість канадської картки в більш ніж 7 мільярдів доларів.

Ідея щодо національної ідентифікаційної картки приваблива на поверхні, але багато країн виявили, що технологія створює більшу кількість проблем, ніж вирішує. Ідентифікаційні картки завжди служили в ролі емоційної політичної відповіді на кризу, але швидкий огляд країн, у яких в недалекі часи було впроваджено ідентифікаційні картки, свідчить, зазвичай, про виникнення низки непередбачених адміністративних і соціальних труднощів. Таїланд, який впровадив свою першу ідентифікаційну картку у 1989 році, після всіх цих років усе ще продовжує згладжувати фундаментальні проблеми.

Жоден уряд все ще не здатен назвати будь-яку країну, де присутність картки утримала б терористів. Для того, щоб досягти такого результату, уряд вимагав би заходів, неймовірних у вільному суспільстві.

Уряди, таким чином, зустрілися з важким вибором. Або вони впроваджують біометричну картку з високим ступенем захисту, що кине виклик кожному принципу свободи, або вони впроваджують картку з низьким чи середнім рівнем захисту, яка буде незабаром доступна злочинцям і терористам на чорному ринку.

Біометричний обман

Усі незалежні дослідницькі студії висунули на перший план величезну прірву між умовами, заявленими біометричними продавцями, і результатом контрольного тестування.

Нещодавнє дослідження Міністерства оборони США виявило, що розпізнавання райдужної оболонки досягло більшого успіху, ніж більшість технологій, але заявка одного виробника на похибку у 0,5 % помилкової ідентифікації, роздулось до 6 % під час іспитів Міністерства оборони [6].

Доповідь, видана Головною лічильною палатою США (US General Accounting Office) в листопаді 2002 року [7], повідомила про те, що найбільша система сканування райдужної оболонки на даний час використовує тільки 30000 записів. Така маленька система діє зовсім іншим чином, ніж система, у яку залучено мільйони чи десятки мільйонів записів.

Головна лічильна палата застерегла, що “невідомо”, яким чином працюватиме система з багатьма мільйонами записів. В доповіді Національного Інституту Науки і Техніки (the National Institute for Science and Technology) [8] робиться висновок, що через недостатню кількість записів і даних неможливо визначити, чи є розпізнавання райдужної оболонки точним способом ідентифікації.

Фундаментальною проблемою для точного функціонування біометрії залишається співвідношення між унікальними біометричними характеристиками особи і кількістю інших ідентичностей, з якими вони співставляються. Це питання простої математики. Якщо біометричне сканування ока чи відбитків пальців один-до-одного відповідає такому ж скануванню, записаному на картку, шанс точної відповідності надзвичайно високий. Похибка може бути встановлена на дуже чутливому рівні (скажімо, плюс-мінус один відсоток). Однак, якщо результат сканування ока співставляється із, скажімо, сотнею інших ідентичностей (відповідність “один до багатьох”), похибка повинна бути збільшена. Інакше, випадки помилкового відхилення будуть неприпустимі. Якщо сканування ока співставляється з національною базою даних, як це запропонували прихильники канадської системи, похибка буде настільки великою, що зробить систему нічого не вартою.

Саме тому математично і технічно неможливо побудувати і використовувати національну базу даних біометричних ідентичностей без того, щоб неминуче не створити помилкове відхилення майже в кожному випадку, коли особа використовує цю систему.

Співставлення даних з елементів схеми ідентифікаційних карток

Автоматизований розподіл даних між організаціями може спричинити суттєвий ризик для осіб, надійності інформації, професійної ефективності і чесності, репутації організації і суспільства в цілому [9].

Співставлення даних серед численних агенцій є складною і часто недосяжною метою. Успішна програма співставлення, що включає численні джерела, вимагатиме високочутливого і строгого поєднання основних умов. Серед них – точна структура визначень, архівна чи альтернативна система підтримки однакової цілісності і набір взаємопов’язаних кодів і методів, які гарантують, що інформація не буде зруйнована чи видозмінена.

Може бути гарантовано, що загроза надійності даних помітно збільшиться, коли програми співставлення розвиватимуться у напрямі від простої компанії до численної корпорації. Можна рівною мірою гарантувати, що програма відповідності послідовно зазнаватиме невдачі, якщо вона базуватиметься на логічно виведених чи “м’яких” елементах даних.

Протягом кількох років організації були зациклені на ідеї зведених чи “об’єднаних” ресурсів даних. Це становить серйозну загрозу безпеці даних. Також представляється неминучим, що дані будуть загублені, перекручені, видозмінені чи стануть об’єктом зловживання. Доступ численних агенцій до вразливих даних значно збільшує потенціал неправильного використання інформації завдяки розголошенню внаслідок корупції або через “дірку” в безпеці.

Загроза безпеці зростає по експоненті відповідно до розширення кількості використання даних поза джерелом “першого покоління”. Просте партнерство двох агенцій, що включає необроблені “тверді” дані, зберігає більший шанс підтримки його безпеки і цілісності. Надійність даних значно зменшується, а загрози її безпеці значно збільшуються з кожним новим застосуванням даних.

Агенції, що використовують систему відповідності різних джерел, можуть зіштовхнутися з істотним інформаційним перевантаженням. Це особливо має місце у справах щодо здоров’я, соціальної допомоги і захисту дітей, там, де потреба підкріпляти, підтверджувати і відсіювати дані для визначення правильності ідентичностей і подій може створити значну загрозу і більш серйозне робоче навантаження, ніж те, яке існує в неавтоматизованій системі.

Співставлення даних також створює загрозу внутрішньому розвитку організацій. Це особливо має місце в сферах діяльності, що вимагає постійних змін і оцінювання, на кшталт тієї, яка існує в сферах освіти і здоров’я. Режим співставлення може стати центром тяжіння, гальмуючи

процес розвитку і створюючи непотрібні загрози стабільності організаційних відносин і обґрунтованості процедур.

Ідентифікаційні картки і крадіжка ідентичності

На перший погляд, видається логічним доводити, що високоінтегрована система ідентифікації допоможе побороти крадіжку ідентичності. Існує, однак, суттєвий масив доказів для того, щоб продемонструвати, що встановлення централізованої ідентифікації може збільшити кількість випадків крадіжки ідентичності.

Найяскравіший приклад такого зв'язку існує в Сполучених Штатах, де НСС став центром ідентифікації і центральним контрольним пунктом реєстру і зв'язку з ідентичністю. Одержання НСС особою передбачає єдиний інтерфейс для взаємодії цієї особи з величезною кількістю приватних і державних організацій. Отже, рівень крадіжки ідентичності в США є непропорційно високим.

Ця ситуація застосовна, однаково, в Австралії, де впровадження Номера Податкового Досьє також збільшило сферу поширення крадіжок ідентичності понад рівень, засвідчений у Великій Британії та інших країнах, в яких відсутня така централізована кодова система.

Ключовий елемент, що сприяє крадіжці ідентичності, – широка доступність центрального номера, пов'язаного з набором персональної інформації. Організації захисту споживачів у США нещодавно розкритикували Комітет Сенату з банківської справи за провал впровадження заходів, спрямованих на цілковиту зміну цієї тенденції. Спілка Споживачів доводить, що крадіжка ідентичності продовжуватиме зростати, поки зв'язки між НСС і публікацією персональних деталей у секторі фінансів не будуть зменшені [10].

Вартість

Наші оцінки загальної вартості Канадської національної ідентифікаційної картки засновані на цілій низці критеріїв. Вони включають (однак не обмежуються):

- створення повної інфраструктури інформаційних технологій;
- вартість самих карток, враховуючи, за оцінкою, три заміни картки протягом життя;
- узгодження публічного і приватного секторів;
- навчання;
- процедури реєстрації біографії;
- встановлення альтернативних і архівних систем;
- механізм зчитування картки;
- умови співставлення даних;
- витрати, що стосуються регулюючих процедур;
- експлуатаційні витрати, включаючи обслуговування і діяльність інфраструктури;
- витрати на додатковий персонал;
- систему співставлення даних, яка пов'язана з реєстрацією карток системи.

У своїх недавніх консультаційних документах щодо впровадження “Карт уповноваження” уряд Великої Британії оцінив, що базова вартість смарт-карток з біометричними даними коштуватиме приблизно 3,2 мільярди фунтів (7,2 мільярда канадських доларів).

Це число повинне бути скореговане з тим, щоб відобразити менше населення Канади (приблизно 50 відсотків населення Великої Британії). Слід додати межу в 10 відсотків, представлену менш сприятливим обсягом економіки.

Таким чином, за британськими параметрами офіційних базових оцінок, канадська картка коштуватиме 4 мільярди канадських доларів.

Однак, оцінки Великої Британії не включають низку ключових витрат, а саме:

- вартість трьох замін картки протягом життя;
- узгодження з приватним сектором;
- повну вартість процедур реєстрації біографії;
- встановлення альтернативних і резервних систем;

- витрати стосовно регулюючих процедур.

Найбільш точні витрати на узгодження приватного сектору були вираховані Австралійськими індустріальними групами (Australian industry groups), які оцінили, що витрати на узгодження з приватним сектором складуть, принаймні, п'ятдесят відсотків від повної експлуатаційної вартості карткової системи.

Архівні системи, що були б потрібні як основний модуль карткової системи, додадуть до повної вартості ще двадцять відсотків.

Компонент додаткових карток і заміни карток включатиме витрати, які становитимуть приблизно тридцять відсотків від вартості початкової реєстрації і вартості управління.

Разом з іншими категоріями, ці результати в сукупності складають 7 мільярдів канадських доларів для національної ID системи.

[1] [//www.news.bbc.co.uk/1/hi/technology/3003571.stm](http://www.news.bbc.co.uk/1/hi/technology/3003571.stm).

[2] [//www.silicon.com/news/500013/1/6129.html](http://www.silicon.com/news/500013/1/6129.html)

[3] Ризики Національних посвідчень особи; Communications of the ACM No 44, 12 грудня 2001 [//www.csl.sri.com/users/neumann/insiderisks.html](http://www.csl.sri.com/users/neumann/insiderisks.html).

[4] Біометрія: використання і зловживання; Communications of the ACM, № 42; 8 серпня 1999 [//www.csl.sri.com/users/neumann/insiderisks.html](http://www.csl.sri.com/users/neumann/insiderisks.html).

[5] [//www.privacyinternational.org/issues/idcard/index.html](http://www.privacyinternational.org/issues/idcard/index.html).

[6] [//www.news.bbc.co.uk/1/hi/technology/3003571.stm](http://www.news.bbc.co.uk/1/hi/technology/3003571.stm).

[7] Повідомлення Генеральної лічильної палати США щодо безпеки кордону [//www.gao.gov/new.items/d03546t.pdf](http://www.gao.gov/new.items/d03546t.pdf).

[8] [//www.itl.nist.gov/iad/894.03/NISTAPPNov02.pdf](http://www.itl.nist.gov/iad/894.03/NISTAPPNov02.pdf).

[9] Роджер Кларк. Комп'ютерна відповідність урядових агенцій: невдача аналізу вартість/вигода як механізму управління [//www.anu.edu.au/people/Roger.Clarke/DV/MatchCBA.html](http://www.anu.edu.au/people/Roger.Clarke/DV/MatchCBA.html).

[10] Заява Союзу Споживачів [//www.consumersunion.org/pub/core_financial_services/000407.html](http://www.consumersunion.org/pub/core_financial_services/000407.html).

*Переклад з англійської Р. Тополевського
//“Свобода Висловлювань і Приватність” • 2004 • 01, 10.09.2004*

~~~~~ \* \* \* ~~~~~