

УДК 681.3.06

Клімушин П. С.,

кандидат технічних наук, доцент,

доцент кафедри інформаційних технологій факультету № 4

Харківського національного університету внутрішніх справ

Білобров А. В.

курсант 2 курсу факультету № 4

Харківського національного університету внутрішніх справ

БАЗОВІ ПРИНЦИПИ ТА ІНСТРУМЕНТИ ЗАБЕЗПЕЧЕННЯ БЕЗПЕКИ Е-ІДЕНТИФІКАЦІЇ ГРОМАДЯН

Застосування інструментів е-ідентифікації громадян необхідно вести на основі таких базових принципів, сформованих на базі найкращих світових практик [1]:

– *адекватність вимог*, тобто використання методу ідентифікації має відповідати меті його застосування (чим менше значущість трансакції з погляду зміни прав громадянина або організації, тим простіші ідентифікатори слід застосовувати);

– *децентралізація та диверсифікація* – системи ідентифікації мають передбачати можливість застосування різних способів виконання операції та не повинні бути прив'язаними до єдиного рішення (наприклад, до універсальної е-картки) або до якоїсь централізованої бази ідентифікаторів;

– *індивідуальний вибір* – система ідентифікації повинна пропонувати користувачеві засоби вибору й контролю тих ідентифікаційних даних, які він надає для різних трансакцій, взаємодіючи з різними відомствами;

– *роз'яснення наслідків* – користувачів необхідно попереджати про те, які їхні ідентифікаційні дані і для чого буде використано в інформаційних системах е-уряду;

– *контроль розповсюдження* – доступ державних відомств до трансакцій в недержавних інформаційних системах (наприклад, платіжних),

розроблених на основі загальних ідентифікаційних даних, можливий тільки за рішенням суду або в інших законодавчо встановлюваних випадках.

З урахуванням цих принципів і найкращих світових практик е-ідентифікації громадян повинні передбачати підтримку декількох незалежних варіантів ідентифікації з можливістю вибору користувачем найбільш зручного варіанта. Тобто єдина е-картка повинна розглядатися тільки як один із інструментів ідентифікації. Система ідентифікації повинна передбачати можливість поділу транзакції на кілька асинхронних сесій, у яких можуть використовуватись різні засоби ідентифікації.

Е-картка повинна бути захищеною від зміни носія інформації, на якому розміщено довірені облікові дані, спеціалізоване програмне забезпечення, прикладне програмне забезпечення (додатки), а також графічні (візуальні) дані, що розміщуються на поверхні картки.

Розширення сфери застосування картки до універсального посвідчення особистості стримується у світі двома факторами: недостатньою поширеністю інфраструктури прийому таких карток; ризиками, що пов'язані з інформаційною безпекою і недостатньою надійністю захисту персональних даних.

Щоб зняти ці ризики, у світі використовують кілька способів. Одним із них є зберігання персональної інформації безпосередньо на картках без створення централізованих реєстрів громадян. Державні установи надають послуги, щоразу дізнаючись персональних даних від самого громадянина, і не мають доступу до даних, контроль над якими міг би становити загрозу для свободи громадян. Персональні дані записуються на картку з використанням криптометодів, що забезпечують виключення несанкціонованого читання і збирання даних.

Зазначені вище ризики об'єднуються, якщо в одній картці поєднуються функції посвідчення особистості з функціями доступу до транзакцій. Така картка в разі її втрати відкриває для зловмисника можливість "крадіжки особистості", а також відкриває перед непідконтрольними користувачами

можливості з втручання в життя громадян. У випадках, коли доступ до картки отримує особа, пов'язана з іноземними державами, такі картки можуть становити загрозу і для національної безпеки.

Держави – члени ЄС мають широкий спектр заходів політики щодо ідентифікаційних е-карток. Такі документи є обов'язковими у восьми державах – членах ЄС. При цьому вони використовуються як засоби е-ідентифікації для отримання онлайн-сервісів від держави [2]. На сьогодні загальний принцип необов'язковості отримання цифрового посвідчення особи є загальноприйнятим. Важливо відзначити, що всі країни, що реалізували проекти упровадження універсальних е-карток, які суміщують функції посвідчення особи і доступу до транзакцій, мають внутрішньополітичну стабільність, відносно невелике населення і є компактними в територіальному плані.

Більшість держав – членів ЄС використовують засоби е-ідентифікації, специфічні для бізнес-установ. Більшість із цих засобів є апаратними ключами, що містять кваліфікований сертифікат для е-підпису. Ці засоби е-ідентифікації можуть використовуватися не тільки для автентифікації, а й для підписання документів від імені компанії. Слід зауважити, що, хоча ці засоби е-ідентифікації можуть використовуватись виключно для представлення компанії, вони є номінативними, тобто містять ідентифікаційні дані представників.

Список бібліографічних посилань

1. Клімушин П. С. Стратегії та механізми електронного урядування в інформаційному суспільстві: монографія. Харків. Вид-во ХарPI НАДУ «Магістр», 2016. 524с.

2. Національна стратегія електронної ідентифікації України. Біла книга з електронного урядування / під редакцією О. Потія та Ю. Козлова. URL : http://dknii.gov.ua/sites/default/files/wb_eid_20_03_0.pdf.