Аналітичний огляд
Сучасні програми розвитку Е-Уряду

к.ф.-м.н. Мартиненко С.В

Анотація

Ця публікація висвітлює сучасні програми розвитку електронного уряду (Е-Уряду) в ЄС з метою врахування їх в програмах розбудови Е-Уряду в Україні. Наведено найбільш вагомі напрямки розвитку, а саме, програми ЄС: «Електронний паспорт», «Електронна митниця», «Електронне голосування». Розглядається питання забезпечення інформаційної безпеки в цих програмах розвитку Е-Уряду.

1. Вступ

Результати Європейської Ради в Лісабоні (березень 2000 р.) встановили нову стратегічну мету для Євросоюзу: отримати в межах десятиріччя саму конкурентну та динамічну інтелектуальну економіку, здатну підтримувати економічне зростання з більшими та кращими робочими місцями і більшою соціальною єдністю. Керуючись цією метою, ЄС вважає за необхідне розвиток програми «Електронна митниця» (Резолюція Ради ЄС від 5 грудня 2003 про створення простого та безпаперового оточення для митниці та торгівлі, 2003/C 305/01).

Програма «Електронний паспорт» може розглядатися самостійною програмою, яка вимагається Міжнародною організацією Цивільної Авіації (ICAO, International Civil Aviation Organisation) та затверджена Постановою Ради ЄС від №2252/2004 від 13 грудня 2004 року. Але ця програма може також розглядатися як складова інших програм, т.я. може забезпечити засобами електронної ідентифікації особи, що можуть бути використані іншими програмами.

Програма «Електронне голосування» є подальшим розвитком програми Е-Уряд. Програма Е-Уряду є більше наданням державних послуг, але Інтернет пропонує можливості розширити участь громадян в управлінні, через електронне голосування (eVoting), яке є, таким чином, інтегральним показником розвиненості Е-Уряду, як показник рівня електронної демократії (E-Democracy). Програми E-democracy прагнуть узяти другий пріоритет у галузі надання державних електронних послуг громадянам.

Всі зазначені програми можуть розглядатися як складові єдиної програми «Е-Уряд», т.я. можуть (і повинні) використовувати спільні ресурси, стандарти, певні дані тощо. Зокрема, програма «Електронна митниця» повинна використовувати технічну базову реалізації програми Е-Уряду, а також забезпечувати сумісність (можливість обміну даними) з іншими державними установами (адміністраціями) або агентствами, залученими до руху товарів в межах кожної держави.

2. Програма «Електронний паспорт» (ePassport, Е-Паспорт)

2.1. Основи програми

В 1968 ICAO (Міжнародною організацією Цивільної Авіації, International Civil Aviation Organisation) почала роботи з визначення специфікацій та всесвітнього Стандарту для машинно-читаємих паспортів, під якими розуміються електронні паспорти з біометричними атрибутами власників (фото, відбитки пальців тощо).

Реалізація стандарту ICAO розроблена для того, щоб «мінімізувати затримки на прикордонних формальностях та захистити операції міжнародної цивільної авіації від незаконного вторгнення», - згідно з д-ром Assad Kotaite, Президентом Ради ICAO.

11 липня 2005 ICAO формально затвердив специфікації машинно-читаного паспорта, розроблені разом з Організацією Міжнародних Стандартів (ISO), як всесвітній стандарт для паспортів. Формальне затвердження також охоплює специфікації, що управляють випуском нової версії стандартизованого паспорта високої безпеки, біометричного паспорта, або «ePassport». Із затвердженням специфікацій як міжнародного стандарту, всі 188 країн, членів

ICAO, погодилися випустити їх паспорти, включаючи нову версію ePassport відповідно до Стандарту не пізніше, ніж 1 квітня 2010 – хоча в більш ранні терміни, до кінця 2006 жовтня, планують реалізувати ePassport понад 40 країни. Зокрема:

- Евросоюз зобов'язав усі 25 Держав Членів мати цілком сумісні ePassports, які містять біометричне зображення обличчя, до вересня 2006 (цей план поки що не виконано);
- Сполучені Штати зобов'язали усі 27 безвізових націй (ті країни, чиї громадяни можуть подорожувати в США без візи США випустили ePassport, сумісний з Стандартом ICAO, до 26 жовтня 2006 року.

Відомий як "ICAO Blueprint" (ICAO проект) мандат специфікацій ePassport:

- фото особи є основним/первинним обов'язковим біометричним параметром; з додатковими (не обов'язковими) параметрами - райдужна оболонка (ока) чи відбитком пальця(ів), як вторинний біометричний параметр;
- безконтактний чип інтегральної схеми, вбудований в ePassport як носій даних;
- глобальна логічна структура даних для програмування чипу; та
- модифікована схема інфраструктури відкритих ключів (PKI).

Вимоги Міністерства внутрішньої безпеки США (Department of Homeland Security, DHS) до паспортів громадян країн, які мають право безвізового в'їду на територію Америки:

- з 26 червня 2005 р. громадяни цих країн, яка приїжджають до США, повинні представлять машино-читаємий закордонний паспорт;
- з 26 жовтня 2006 р. цей паспорт повинен містити цифрову фотографію власника, а також закордонний паспорт повинен містити мікросхему (чип), яка здатна зберігати в своїй пам'яті біографічну інформацію з відповідної сторінки паспорта, цифрову фотографію та іншу біометричну інформацію.

На 7-й семінарі в Ісландії 26–27 травня 2005 Міжнародної Групи Porvoo, яка була створена в зв'язку з проектом ЄС eEurope, біля 80 представників 18 європейських країн, Японії та США, а також представники Європейської Комісії та Об'єднаних Націй, обговорювали ситуацію щодо Європейського електронного посвідчення особи (Е-Паспорт) та електронних послуг і проектів розвитку, а також обміну інформацією щодо проектів.

Зокрема, були сформульовані три головні задачі політики Е-Паспорту:

- розширене використання сертифікатів PKI (Public Key Infrastructure);
- відкритий та стандартизований ринок, який забезпечує сертифікати та пов'язані послуги;
- повна сумісність з ЄС - та міжнародними стандартами, що таким чином забезпечить сумісність з адміністраціями інших країн.

Відповідні стандарти ЄС затверджені Постановою Ради ЄС від 29.12.2004 (Council Regulation (EC) on standards for security features and biometrics in passports and travel documents issued by Member States, Official Journal L 385 , 29/12/2004 P. 0001 – 0006).

2.2. Стан програми Е-Паспорт в ЄС

Відповідно до вимог Європейської Комісії, Дирекції Загальної юстиції, Свободи та Безпеки, в Е-Паспорті ЄС фотографія особи стає обов'язковою з серпня 2006 року.

Англія. Є велика кількість ініціатив в області електронного посвідчення особи (ID картах) щодо ліцензування водіїв. Плани по національних ID будуть затверджені законопроектом, який очікується прийняти в кінці 2005, з реалізацією протягом 2008–2009. Карти ID будуть засновані на паспортах і біометриках, та зберігатимуть ключовий компонент (ключ електронного підпису).

Бельгія. Пілотний проект розпочато з вересня 2004. Мета - замінити паперові посвідчення особи на електронні в кінці 2009, носіння яких (при собі) ID обов'язкове. Інфраструктура відкритих ключів PKI підтримує механізм електронного підпису, який може використовуватися і для послуг електронних транзакцій. Відповідальний Центр сертифікації ключів - це напів-приватна організація. Бельгія, ймовірно, перша країна в світі, яка завершить упровадження ICAO-сумісних електронних паспортів Е-Паспорт. З 30 січня 2005 всі нові паспорти випускаються за технологією безконтактного чипа. В цілому випущено більш 150,000 Е-Паспортів. Бельгійський паспорт одержав від Інтерполу в 2003 нагороду «найбезпечніший паспорт світу».

Подальший розвиток включає онлайн веб-вузол www.diplomatie.be/passweb, на якому може перевірятися статус бельгійського паспорта. Цей веб-вузол пов'язаний з централізованою електронною базою даних вкрадених і втрачених паспортів, які доступні кожній урядовій службі або навіть приватним особам. Будь-які запити до цих файлів належним чином реєструються. Бельгія має суворе законодавство про конфіденційність. Крім того, кожний громадянин може подивитися в онлайні, хто заглядав в його/її файл, і якщо необхідно може сформувати файлом скаргу.

Естонія використовувала електронні ID карти з 2002, носіння яких (при собі) обов'язкове. Національні ID карти випускаються Комісією/ Палатою Громадянства і Міграції. Понад 100 послуг можуть використовуватися з цією картою. Другий чип, що містить біометрію, зображення особи і відбитки пальців, відповідно до стандартів ICAO, буде додано до цієї карти. Естонська ініціатива розглядається Бельгією і Фінляндією.

Ісландія має на меті випустити перші біометричні паспорти в жовтні2005. Політика сертифікатів уряду Ісландії заснована на європейському стандарті ETSI TS 102 042 і OCES політиці сертифікатів Данії.

Італія у березні 2005 схвалила національний закон, згідно з яким стане обов'язковим випускати громадянам посвідчення особи тільки в електронній версії, які громадяни будуть застосовувати, починаючи з 1-го 2006 січня. Передбачається використовування біометрії (один відбиток пальця, разом з фото власника). Найвища задача італійського уряду по введенню електронного посвідчення особи - захист прав громадян; конфіденційність даних громадян.

Литва підготувала введення нового не-біометричного паспорту (виготовлено 1 млн.штук).

Польща утримується від біометричних документів до 2007 через проблеми коштів.

Нідерланди: з вересня 2004 до лютого 2005мало місце шестимісячне випробування Е-Паспортів в шести голландських муніципалітетах, де разом було випущено 14,700 Е-Паспортів. Випуск нового паспорта почнеться осіню 2006 року.

Німеччина. З різних проектів карт, за які відповідальним є Федеральний Уряд, зараз головний пріоритет віддано Е-Паспорту. Розгортання процесу ICAO-сумісних паспортів передбачено почати в листопаді 2005. Додатково, німецький Федеральний Уряд стартував ініціативу eCard. Мета цієї ініціативи - визначення та реалізація загальної платформи для всіх інтелектуальних карток, що розвиваються в Німеччині, включаючи ті, за які будуть відповідальні міністерства Федерального Уряду (наприклад, медична карта, карти державного службовця, робоча картка/ трудова книжка) та приватні пропозиції у сфері банківських карт, які відносяться до «альянсу електронний підпис». Е-Паспорти передбачається вводитися в 2007 з використанням як в приватних, так і державних послугах, здебільшого для доступу до послуг Е-Уряду.

Норвегія. З 1975 банки в Норвегії встановили загальні системи для банківських ідентифікаційних карт. Банківська мережа стала дуже популярною, і банки розробляють загальну міжбанківську електронну систему посвідчення особи.

Словаччина. Словацький уряд оголосив про плани запустити випуск біометричних паспортів з 1 вересня 2006 року.

Фінляндія. Випуск електронних ID карт був розпочатий в 1999. Карта містить цивільне посвідчення, випущене Центром Реєстрації Населення, який є сьогодні єдиним емітентом якісних сертифікатів у Фінляндії. Карта ID не обов'язкова. Електронний підпис вже використовується. Є більше 50 послуг, які використовують карту, включаючи Податкову Адміністрацію, послуги страхових компанії, установи Соцстраху, електронний сервіс Фінляндії та фінські Сили Оборони (список послуг доступний на www.etu-klubi.fi). Для взаємного розпізнавання електронних ID карт, Фінляндія вступила в угоду кооперації з Естонією в 2003. Впровадження біометричних ID карт передбачається в 2007–2008. У Фінляндії відповідальним за біометричний проект є Міністерство Внутрішніх справ. Мета - стартувати випуск ePassports весною 2006.

Франція. Задача французької адміністрації - зберегти/ забезпечити зближення з німецькими специфікаціями, щоб дозволити ступінь сумісності для обох платформ, які складають основу майбутнього стандарту для європейської Цивільної Карти. Необхідно ухвалити рішення щодо того, чи будуть електронні ID обов'язковими у Франції, чи залишаться додатковими, як вони є сьогодні. Електронний підпис вже використовується у Франції для деяких додатків, але ще не здійснюється у великому масштабі або для цілей електронного посвідчення особи.

Швеція. Мета уряду - надати громадянам цілодобові (24x7) «комплексні е-послуги» (“one-stop-e-services”) з використанням стандартизованого електронного Е-Паспорту. Інфраструктура може також використовуватися приватними акціонерними компаніями. На сьогодні відповідальні Центри сертифікації - це шведські банки і телекомунікаційний оператор TeliaSonera. Е-Паспорт не обов'язковий в Швеції.

Приклади електронних послуг, які тепер доступні утримувачам, включають послуги шведського Податкового Агентства, Пенсійної служби, реєстрації нової адреси, дозволи заснувати корпорацію вантажівок, таксі або іншу транспортну корпорацію, оновлення банківських позик і велике число електронних послуг місцевого управління. Шведська Асоціація Постачання Фермерів та Маркетингу Урожаю також буде використовувати Е-Паспорт для укладання контрактів між орендарями і асоціацією.

У жовтні 2005 поліція почне випуск національної електронної ID карти, яка буде як офіційним ідентифікаційним документом, так і шведським паспортом.

3. Програма «Електронна митниця» (eCustoms)

Нормативні документи ЄС щодо побудови системи «Електронна Митниця» (Е-Митниця):

- **Рішення** № 253/2003/ЕС Європейського Парламенту та Ради від 11 лютого 2003 про ухвалення програми заходів для митниці в Співтоваристві (Митниця 2007);
- **Резолюції Ради ЄС** від 5 грудня 2003 про створення простого і безпаперового оточення для митниці та торгівлі (2003/С 305/01);
- **Повідомлення** Комісії для Ради, Європейського Парламенту та Європейського Економічного і Соціального комітету про просте і безпаперове оточення для Митниці та Торгівлі від 24.07.2003, COM(2003) 452 final, 2003/0167 (COD);

- Проект Е-Митниця бачення і багаторічний стратегічний план, Європейської Комісії TAXDU/477/2004 від 20.10.2004;

- **Повідомлення** Комісії для Ради, Європейського Парламенту та Європейського Економічного і Соціального комітету та Комітету регіонів про роль Е-Уряду для європейського майбутнього 26.9.2003, COM(2003) 567 final.

Мета програми Е-Митниця визначена в Резолюції Ради ЄС від 5 грудня 2003, зокрема:

«глобалізація та лібералізація торгівлі, значне зростання об'ємів торгівлі та приріст e-commerce і обширне використання інформаційної технології кидають новий виклик митним органам; таким чином необхідно, щоб митниці власті забезпечували більш ефективні та дружні електронні послуги для того, щоб просувати європейську конкурентоспроможність».

Згідно з Проектом Е-Митниця від 20.10.2004 Комісія та Держави Члени націлюватимуться на вирішення до 2008 року таких задач:

- обмін електронний даними між митними управліннями можливий в межах усього Співтовариство, що вимагається для будь-якої митної процедури або будь-якої іншої мети (наприклад, декларації перед-прибуття);
- імпортер може подавати його короткий звіт та/або митну декларацію в електронній формі для зазначеного вище, незалежно від Полягання Члена, в якому товари вступають/входять в Співтовариство;
- експортер може подати його експортну декларацію в електронній формі для зазначеного вище, незалежно від держави-члена, від якій товари залишають Співтовариство;
- збори та оплата/звільнення мит за імпорт, у принципі, буде оброблена митним управлінням, відповідальним за місце, де імпортер/експортер зареєстрований та утримуються його митні записи;
- набір товарів для митного контролю прикордонних та внутрішніх митних офісів заснований на аналізі ризику, що використовується міжнародними, Співтовариства та національними критеріями, критеріями Співтовариства, якими держави-члени обмінюються електронним способом;
- Авторизовані Економічні Оператори (AEO - Authorized Economic Operators), включаючи митних агентів, можуть, в їх запиті, діяти в межах всього Співтовариства на підставі єдиного уповноваження/авторизації, наданого згідно з встановленими критеріями Співтовариства; це включає використання допомоги, загальної довідкової системи для операторів і загальних якісних стандартів, а також і існування загальної бази даних AEO, доступної митним управлінням/офісам в межах всього Співтовариства;
- трейдери мають доступ до інформаційного порталу та єдиної точки електронного входу/доступу для імпортних і експортних операцій, незалежно від держави-члена, в якому починаються операції або закінчуються, і навіть, якщо операція залучає агентства, окрім митниці (єдине вікно, універсальний магазин).

В цілому багаторічний стратегічний план для eCustoms розбивається на такі категорії (по роках) для держав-членів:

1. законодавчі зміни і спрощення **(2003-2007)**,
2. операційна конвергенція/зближення **(2003-2005)**, і
3. комп'ютеризація митних процесів **(2004-2009)**.

План програми ЄС «Електронна Митниця» включає створення таких проектів комп'ютеризованої системи (по роках) для Держав Членів:

- Автоматизована Система Експорту (AES) **(2003-2007)**
- Автоматизована Система Імпорту (AIS) **(2004-2009)**
- Обмін інформацією щодо ризику **(2004-2007)**
- База(и) даних AEO (Авторизованих Економічних Операторів) **(2005-2009).**

В межах кожної держави необхідно виконати:

- сумісність митних органів з іншими державними органами або агентствами, залученими до митних операцій в межах тієї ж Держави Члена **(2004-2007)**

Етапи робіт загальної системи ЄС:

- загальний (ЄС) портал інформації митниці для трейдерів **(2004-2010)**
- єдина точка (ЄС) електронного доступу/входу до операцій **(2004-2010)**

Щодо технічної реалізації програми зазначеними документами вимагається, зокрема:

- в Повідомленні Комісії COM (2003) 452 (п.*4.1.8. Електронний підпис, електронні документи, електронний архів*) зазначається, що використання інформаційних технологій формулює **критичну проблему достовірності та цілісності** даних, якими обмінюються та зберігають електронним способом. Електронний підпис призначається для засвідчення персони, яка підписала електронний документ.

- вже прийнято відповідне законодавство Співтовариства, щоб гарантувати законодавчий статус електронних підписів – це Директива 1999/93/ЕС та ін. Тому Держави Члени повинні в Митному Кодексі чітко визначити законодавчий статус електронного підпису та електронного документу для митниці, незалежно від стану реалізації в різних Державах Членах; **та гарантувати сумісність використання електронного підпису**.

- відповідно до Резолюції Ради ЄС від 5 грудня 2003 про створення простого і безпаперового оточення для митниці та торгівлі (2003/C 305/01), необхідно «розглядати, в кооперації з Комісією, загальні/спільні рішення, які дозволять **сертифікацію і схвалення електронного підпису, незалежно від Держави Члена**, в якій заснований економічний оператор».

- **технічною базовою основою реалізації програми «Електронна Митниця» є** прийняття Державами Членами ЄС зобов'язань щодо структури Електронної Європи (e-Europe) та, зокрема, Е-Уряду.

Реалізація програми eCustoms в ЄС розпочата в 2003 році через пілотний проект Системи Експортного Контролю (ECS), в якому беруть участь 12 (із 25) Держав Членів (Бельгія, Німеччина, Італія, Іспанія, Швеція, Сполучене Королівство, Чеська Республіка, Данія, Португалія, Нідерланди, Австрія, Польща).

4. Програма «Електронне голосування» (eVoting, Е-Голосування)

4.1. Основи програми

Виборчі питання були предметом неодноразового обговорення Парламентської Асамблеї ЄС, зокрема ряду докладів так званої Венеціанської комісії Ради Європи - «Європейська комісія за Демократію через Право» (Венеціанська Комісія) (European Commission for Democracy through Law - Venice Commission), присвячених проблемам відповідності віддаленого голосування (голосування поштою або електронне голосування) стандартам Ради. Доклад був схвалений Радою 12-13 березня 2004 року.

Відзначаючи, що деякі країни вже використовують Е-Голосування або планують це робити, і підкреслюючи вигоди, які надає Е-Голосування, Комісія проте попередила про необхідність вжиття певних заходів захисту, які покликані мінімізувати ризик фальсифікацій.

Комісія визначила 5 принципів, які відображають засади європейської демократії та однаково придатні як для виборчих компаній, так і для референдумів:

- *Універсальне право голосу:* всі люди мають право голосу та підтримку вибору кандидата на визначених умовах, наприклад, віку та громадянства.
- *Рівні права голосу:* кожен виборець має рівне число голосів.

- *Свобода права голосу*: виборець має право сформувати та виявити власну думку у вільній формі, без будь-якого примушення або впливу.
- *Таємність права голосу:* виборець має право вибирати таємно як особистість, та мати спроможність обов'язково захистити це право.
- *Пряме право голосу:* вибір (балотування), зроблений виборцями, безпосередньо визначає вбрану(их) особу (або осіб).

У зв'язку з цим, Комісія рекомендувала наступне:

- Е-голосування може використовуватися лише за умови, що система є безпечною/захищеною (тобто, в змозі витримати сплановану/навмисну атаку) і надійною (тобто, здатна нормально функціонувати незалежно від проблем з програмним забезпеченням, устаткуванням, живленням і т.п.);

- Система Е-Голосування повинна бути прозорою, тобто надавати можливість перевірки її функціонування, у тому числі, система має бути відкритою з точки зору методів та рішень, які в ній застосовуються;

- Виборці повинні мати нагоду одержати підтвердження свого вибору і виправити його, у разі помилки. При цьому не повинен порушуватися принцип таємності голосування;

- Для полегшення перерахунку голосів у разі конфліктної ситуації може передбачатися процедура роздруку голосів в спеціальні бюлетені і їх подальше зберігання в спеціальних контейнерах.

Комісія прийшла до висновку, що при дотриманні вказаних умов електронне голосування не суперечить положенням «Кодексу правил належної практики виборів» 2002 р. Європейської комісії за Демократію через Право (Венеціанська Комісія) та європейській Конвенції про права людини.

Таким чином, прийнятність систем Е-Голосування визначається правовими, процедурними і технологічними стандартами, які використовуються в процесі голосування та забезпечують зазначені вимоги.

4.2. Безпека Е-Голосування

Для забезпечення безпеки систем Е-Голосування в США були розроблені відповідні стандарти - VSS (Voluntary Voting Systems Standards). Ці стандарти розроблялися для системи голосування DRE (direct-recording electronic — «електроніка прямого запису») з перфокартами та оптичним скануванням. Оновлена версія стандартів (Federal Election Commission, *Voting Systems Performance and Test Standards,* 30 April 2002, http://www.fec.gov/pages/vssfinal/vss.html) включає розділ по безпеці (том 1, розділ 6).

Разом із стандартами, розроблялися та управлялися Національною Асоціацією Державних Виборчих Директорів (NASED, National Association of State Election Directors) добровільне тестування та програма видачі свідоцтва (сертифікація). В цій програмі Незалежний центр тестування (ITA, Independent Test Authority), вибраний NASED, тестує системи Е-Голосування та підтверджує (сертифікує) на відповідність стандартам VSS. Тестування підлягають як технічні засоби, так і програмне забезпечення, і перевірене програмне забезпечення і пов'язана документація зберігається в ITA. Якщо виникають питання чи було спотворене програмне забезпечення, що використовується у е-виборах, то код може порівнюватися з версією, яка зберігається в ITA.

Законом HAVA (Help America Vote Act of 2002) США була створена Комісія сприяння виборам (EAC, Election Assistance Commission) для заміни FEC (Federal Election Commission), EAC була створена в 1990 та встановлює три органа, підпорядкованих EAC:

- 110-членів Ради стандартів (Standards Board), що складається з державних і місцевих посадовців виборчих органів;

- 37-членів Ради консультантів (Board of Advisors), що представляють доречні організації та асоціації в області науки і технологій;
- 15-членів Комітету з розробки технічних керівництв (Technical Guidelines Development Committee) під головуванням директора Національного Інституту Стандартів і Технологій (NIST). Цьому Комітету доручається створення рекомендації щодо стандартів добровільної дії (головні принципи яких викладені в Законі HAVA), які потім переглядаються двома Радами та EAC.

Закон HAVA також вимагає від EAC забезпечення тестування, видачі сертифікатів та позбавлення сертифікації систем голосування, залучення NIST та контроль вибраних тестових лабораторій. Також вимагається, щоб EAC проводив вивчення проблем і звернень, включаючи потенційно можливі шахрайства, пов'язані з Е-Голосуванням.

4.3. Досвід Е-Голосування

Казахстан

Перший крок був зроблений в 2000 році у вересні, коли згідно з Указом Президента було створено Державну урядова робочу групу, що складається з 18 чоловік, і пропонували внести зміни та доповнення до законодавства. В 2003 р. заплановано в бюджеті фінансування Е-Голосування. В 2004 р. закуплено устаткування на 3000 ділянок, проведено навчання операторів. В квітні 2004 р. прийнято зміни до закону про вибори - дев'ятий розділ; внесено доповнення до адміністративного кодексу про відповідальність за злам системи.

Естонія

Електронне голосування через Інтернет відбудеться на міських виборах в Талліні в кінці 2005 року, як прелюдія введення онлайн голосування на парламентських виборах 2007 року.

Подібно більшості інших європейських країн, Естонія має законодавство щодо цифрового підпису, але на відміну від багатьох інших також має законодавство щодо цифрових посвідчень особи (введене ще в 2002 р.) - ID-картки. На додаток до багатьох розширених особливостей захисту, ця картка має машинно-читаємий код і мікрочіп, що містить візуальні дані на картці, а також два цифрових сертифікати, призначених для перевірки особи власника картки та надання цифрових підписів. Можливо, що в майбутньому буде реалізована інтеграція посвідчення особи та банківських карток, як і інших карток спеціального призначення. До травня 2004 р. випущено 500,000 ID-карток.

Отже, звичайний естонець тому має доступ до двох окремих цифрових сертифікатів, заснованих на стандартизованих платформах, які мають урядову підтримку через постачання інструментальних програмних засобів до бізнес-структур і громадян для вільного їх використання. Широке розгортання цифрових сертифікатів, яким довірять, дозволяє використовувати ID-картки у ряді банківських операцій з місцевими сучасними (передовими) банками. На додаток, щоб допомоги створити один із світових ринків електронного банкінгу (e-banking), що розробляється (95% банківських операцій виконуються через цифрові канали), естонський уряд планує використати ID-карти, як засіб для здійснення програми електронної демократії (e-democracy) в 2005 році.

Естонія визнана першою країною Центральної Європи для прийняття національного законодавства з електронного голосування. Пілотні проекти Таллінна є частиною естонського проекту по онлайн голосуванню, розпочатому в серпні 2003 року.

Система онлайн голосування ґрунтуватиметься на інфраструктурі PKI (Public Key Infrastructure), яка дозволяє проводити безпечну ідентифікацію громадян з використанням цифрових підписів і електронних ID карток. На даний більше 1 млн. громадян країни мають електронні картки (більшість потенційних виборців).

США

Різного роду важільні та перфокарточні машини для голосування застосовуються в Штатах вже багато десятиріч, проте як найвірогідніша заміна для застарілої техніки виступає, як правило, саме електронний «чорний ящик», але в більш прогресивному виді сенсорної рідкокристалічної панелі-екрану і реєстраційної смарт-карти виборця.

Виготовляють такі пристрої, що коштують близько 5 тисяч доларів, головним чином дві приватні американські компанії — Diebold і ES&S (Election Systems & Software), які контролюють 80% цього сектора ринку.

Проведення електронних виборів проявило певні проблеми в США. Одна з них – неможливість виборців перевірити свій вибір. Доступно суть проблеми з новою технікою висловлює в своїх виступах конгресмен Раш Холт від штату Нью-Джерси: «уявіть собі день виборів 2004 року. Ви приходите на виборчу дільницю та віддаєте свій голос за допомогою сенсорного екрану новітньої машини для голосування. Екран говорить, що ваш голос врахований. Але покидаючи виборчу кабінку, ви ставите собі питання: а як я власне взнаю, чи вірно машина зафіксувала мій голос? Факти такі, що взнати це неможливо». При реалізованих нині електронних технологіях у виборця в США немає абсолютно ніякої можливості упевнитися, що голос, відданий через сенсорний екран за кандидата А, не приписаний машиною кандидату Б.

Друга суттєва проблема – проблема безпеки. Як говорить Девід Ділл, (David Dill), професор інформатики Стенфордського університету, «все, що ми чуємо в безлічі різних місць, — це те, що не слід хвилюватися з приводу даних машин, оскільки вони сертифіковані на федеральному рівні і рівні штатів. **Проте надзвичайно важко одержати безпосередню інформацію про те, що саме відбувається в ході сертифікаційного процесу**». Одночасно під приводом комерційної таємниці в найстрогішому секреті тримаються і всі подробиці про внутрішній устрій техніки.

Не бажаючи миритися з щільною завісою таємниці навколо машин для голосування, журналістка і суспільна активістка Бев Харріс вже не перший рік веде за допомогою друзів приватне розслідування всієї цієї історії. Підсумком роботи стала книга «Вибори з чорним ящиком: підробка голосування в 21 столітті» (Bev Harris, «Black Box Voting: Vote Tampering in 21st Century. Elon House, 2003, www.blackboxvoting.org). В книзі на основі бесід з конкретними учасниками подій показано, зокрема, **що так звана «сертифікація» електронних машин - це чистий фарс упереміж з відвертою брехнею** (подробиці див. www.scoop.co.nz/mason/features/?s=usacoup).

Індія

Індійська машина для голосування, або EVM (Electronic Voting Machine), - це розроблений в 1989–90 рр. пристрій, що складається з двох модулів - блоку управління і консолі для голосування.

Консоль має список кандидатів, поряд з кожним з яких розташована кнопка реєстрації голосу. Після натиснення на неї пристрій введення блокується до наступного виборця, а зафіксований голос заноситься в елемент пам'яті відповідного кандидата. На блок управління покладені функції загального забезпечення процесу, видачі на дисплей сумарної кількості громадян, які проголосували, опечатування результату після закінчення процедури та фінального оголошення результатів виборів.

З міркувань безпеки електронні машини не під'єднуються ні до яких мереж і центральних баз даних, а підсумки голосування фіксуються членами регіональної виборчої комісії. Завдяки такій простій конструкції електроніка машини для голосування не вимагає ніякої операційної системи, всі коди команд зашиті безпосередньо в мікросхеми, а система з цієї причини вважається надзвичайно стійкою до атак (хакингу).

З точки зору комп'ютерної безпеки індійський варіант EVM є типовим «чорним ящиком», весь захист інформації в якому побудований на основі секретності і складності фізичного доступу до коду.

Добре відомо, що підхід до безпеки на основі концепції «чорного ящика» ненадійний, оскільки дає широкий простір для зловживань.

В тій же Індії, наприклад, ще в 2001 році політична опозиція рішуче виступила проти EVM, **що випускаються державними підприємствами і тими, що знаходяться під контролем «партії влади».** На конкретному прикладі було продемонстровано, що, всупереч завірянням виробників і виборчої комісії про «стійкість машини до хакингу», системна плата легко та без втрат функціональності витягується з корпусу EVM, код мікросхем зчитується, а чіпи можна поміняти на перепрограмовані. У результаті така модифікована машина робить все як і повинна, проте на кінцевому етапі знімає зі всіх елементів пам'яті певну частку голосів і приплюсовує їх до голосів, що «потрібно», гарантуючи перемогу потрібному кандидату і зберігаючи загальне число виборців, що проголосували.

Бразилія-США

Як повідомив офіційний представник Diebold Election Systems, компанія без проблем надасть можливості генерації «паперового сліду» замовникам із США, якщо у тих з'явиться така потреба. Більш того, при експортних поставках Diebold вже забезпечує свої машини можливостями друку контрольних бюлетенів. Зокрема, значна частина з 300 тисяч машин для голосування, проданих до Бразилії, обладнана контрольним принтером по «методу Меркюрі» (в захищеному боксі за склом виводиться квитанція, що засвідчує, що голос виборця врахований, і що залучається до контрольного архіву). Ця техніка успішно випробувана на практиці в ході бразильських парламентських виборів в жовтні 2002 року (www.spectrum.ieee.org/WEBONLY/publicfeature/oct02/evot.html). Про розробку аналогічного пристрою для своїх сенсорних екранів оголосила і фірма ES&S, головний конкурент Diebold.

Австралія

Як насправді повинна проходити подібна модернізація виборів, наочно демонструє Австралія. В 1998 році в цій країні теж відбувся конфуз з традиційними бюлетенями, коли два кандидати набрали практично рівне число голосів, і при декількох підрахунках перевага виявлялася то у одного, то у іншого. В результаті уряд ухвалив рішення про розробку EVACS, Системи електронного голосування і підрахунку голосів (www.elections.act.gov.au/EVACS.html). Процес її створення був повністю прозорий: оголосили конкурс з відомими учасниками і відомим жюрі, а підсумковий продукт віддали на експертизу відомій третій стороні — аудиторській софтверній фірмі BMM International. Нарешті, все програмне забезпечення EVACS написано у відкритих початкових кодах та у вигляді zip-файлу доступно будь-кому для ознайомлення безпосередньо на урядовому сайті.

Як показало опитування 1000 австралійських виборців, яке проведене Виборчою комісією Австралії, більшість громадян цієї країни підтримує введення електронного голосування. В основному за електронну систему виборів висловилися люди у віці від 25 до 34 років, чий річний дохід перевищує 80 тис. австралійських доларів (приблизно 53 тис.$) і які мають домашні комп'ютери та знайомі з системами електронних платежів.

Швейцарія

В Швейцарії провели у вересні 2004 р. референдум з використанням електронного голосування. Більше 2700 з 22000 виборців передмість Женеви проголосували в режимі онлайна. До цього в Швейцарії електронне голосування використовувалося на декількох місцевих виборах. В середньому 90% швейцарських виборців віддають перевагу традиційному методу голосування.

У ході референдуму використовувалося програмне забезпечення, розроблене сумісно з HP і фірмою Wisekey, що спеціалізується в області IT-безпеки. Всі виборці одержали карту з

можливістю вибору 3-х способів голосування. Карта містила 16-значний особистий ідентифікатор і 4-значний код безпеки. Виборці могли відвідати спеціальний веб-сайт, ввести персональний код і одержати бюлетень для голосування, яке здійснювалося шляхом його заповнення, введення коду безпеки та відправки бюлетеня.

Корея

З 2005 року для всіх політичних виборів в Кореї вводиться система електронного голосування, випробування якої почалися 2004 року. Корея стане першою азіатською країною, де голосування на всіх політичних виборах проводитиметься електронним способом.

В дослідному режимі нова система голосування почала функціонувати 2004 року. Згідно з повідомленням газети Korea Herald, уряд дозволить громадянам голосувати через неї з найважливіших політичних питань. Крім того, через Інтернет будуть доступні до 85% державних служб, що на 15% більше, ніж тепер. Служба «одного вікна» у Вебі допоможе організувати реєстрацію онлайн-компаній.

До 2005 року весь державний документообіг буде переведений в цифрову форму, а до 2006 року буде створена база даних основних цивільних документів, що повинне підвищити ефективність роботи уряду і скоротити витрати.

До 2007 року уряд створить національну інформаційну мережу для нагляду за імпортом/експортом, митницями, залізничним та автомобільним транспортом.

Пілотні проекти систем електронного голосування запустили й інші азіатські країни, включаючи Японію, Тайвань і Гонконг. В червні 2002 року жителі міста Ніїмі, розташованого приблизно в 500 км від Токіо, стали першими в Японії «е-виборцями». За повідомленням Associated Press, понад 15 тис. людей зробили свій вибір, прикладаючи пальці до екранів машин для голосування.

5. Висновки

Основними питаннями зазначених програм є питання забезпечення безпеки та уніфікації технічних стандартів, питання законодавства. Тому для успішного розвитку програм необхідно, як мінімум:

1). Затвердити перелік технічних стандартів для кожної з програм. При цьому слід врахувати, що на відміну від програми Е-Голосування, інші програми ПОВИННІ бути сумісні з відповідними європейськими та міжнародними програмами, а отже базуватися виключно на європейських та міжнародних технічних стандартах.

2). Привести у відповідність законодавство України до законодавства ЄС щодо: а) дистанційного (електронного) голосування; б) електронного паспорту; в) Держави Члени повинні в Митному Кодексі чітко визначити законодавчий статус електронного підпису та електронного документу для митниці, незалежно від стану реалізації в різних Державах Членах, та гарантувати сумісність використання електронного підпису.

3). З метою економії коштів, необхідно «поєднати» програму Е-Уряду з програмами Е-Митниця, Е-Паспорт та Е-Голосування, виробивши єдину концепцію та сумісні стратегічні плани розвитку.

4). Створити/ Залучати незалежний (не державний) центр тестування. Так як в Україні неможливо одержати безпосередню інформацію про те, що саме відбувається в ході сертифікаційного процесу безпеки інформаційної системи; так як за цей процес відповідає державний орган, то для таких програм як Е-Голосування повинні залучатися незалежні центри сертифікації (тестування).