УДК 681.323

К.А. ПОГРЕБНЯК, П.О. КРАВЧЕНКО

МОДЕЛЬ КОМБІНОВАНОЇ ІНФРАСТРУКТУРИ ВІДКРИТИХ КЛЮЧІВ

Пропонується модель комбінованої інфраструктури відкритих ключів (ІВК), що поєднує у собі переваги ІВК на базі X.509 та ІВК на базі ідентифікаторів. Особливістю розробленої комбінованої ІВК є наявність відокремленого серверу підпису, який забезпечує цілісність, автентичність, доступність та своєчасне поновлення бази даних ідентифікаторів користувачів домену та загальносистемних параметрів.

Вступ

Як показують дослідження, подальший розвиток електронного документообігу можливий лише за умови суттєвого скорочення витрат на ІВК [1]. На даний момент в Україні ІВК функціонують на національному або регіональному рівні та базуються на використанні сертифікатів відповідно до стандарту X.509 [2]. Використання ІВК на базі X.509 у межах організацій, міністерств та відомств не дозволить скоротити витрати користувачів, оскільки побудова та розгортання такої інфраструктури вимагає значних фінансових затрат. З іншого боку, використання альтернативної ІВК на базі ідентифікаторів дозволяє скоротити витрати на створення, впровадження та користування послугами, що надає зазначена інфраструктура [3]. Однак архітектура ІВК на базі ідентифікаторів потребує довіри до уповноваженого на генерації ключів (УГК), оскільки безпосередньо УГК генерує та видає особистий ключ користувачу. Вимога розповсюдження та можливість зберігання особистих ключів користувачів не дозволяє використовувати ІВК на базі ідентифікаторів на регіональному та національному рівнях.

У науковому співтоваристві з'явилася ідея використання комбінованої ІВК, тобто ІВК на базі X.509 впроваджується на національному та регіональному рівнях, а ІВК на базі ідентифікаторів – на рівні організацій, міністерств та відомств [4].

На даний час запропоновано декілька моделей комбінованих ІВК, що мають за мету спростити процес електронного документообігу за рахунок скорочення кількості сертифікатів користувачів. Розглянемо основні недоліки запропонованих моделей комбінованих ІВК.

Girault [5] будує схему, у якій відкритий ключ ділиться на дві частки, одну з яких виробляє сервер, а іншу – користувач. У такому разі УГК не в змозі підмінити відкритий ключ користувача. Але для того щоб довести справжність відкритого ключа, відправнику необхідно виконати інтерактивний протокол з нульовими знаннями з одержувачем. Зазначена схема передбачає, що відправник та одержувач володіють однаковими загальносистемними параметрами.

У схемі Gentry [6] таємний ключ розділяється на дві частини, однією з них володіє сервер, іншою – користувач. Для розшифрування повідомлення користувач повинен отримати другу компоненту таємного ключа від сервера по захищеному каналу зв'язку. Сервер сертифікує ідентифікатор та відкритий ключ користувача. Таким чином, усі користувачі повинні мати сертифікати.

Al-Riyami та Paterson [7] запропонували схему, дуже схожу на схему Gentry, але у ній немає необхідності сертифікувати відкритий ключ користувача. Користувач публікує дві частки відкритого ключа, які пов'язані між собою. Але сервер генерації ключів може легко скомпрометувати користувача, замінюючи його відкритий ключ, та при цьому ця заміна не може бути ніяким чином виявлена.

Chen у роботі [8] пропонує механізм перевірки відкритих ключів засвідчувальних центрів, що видають особисті ключі. Він показує, яким чином можна побудувати ієрархічну систему, у якій можна перевірити увесь ланцюг сертифікатів. Але поза увагою залишаються питання отримання справжніх ідентифікаторів та загальносистемних параметрів.

Callas [9] запропонував схему, у якій сервер генерує відкрий і таємний ключ кожного користувача. Щоб отримати відкритий ключ користувача, необхідно здійснити неавтентифікований запит до сервера. Для отримання таємного ключа користувача необхідно здійснити автентифікований запит до сервера. Механізми доведення цілісності та справжності видкритого та таємного ключів не уточнюються.

У схемі Voltage [3] користувачі володіють сертифікатом традиційної ІВК та ключем ІВК на ідентифікаторах. Сертифікати використовуються для автентифікації користувача та для накладання цифрового підпису, ключі ІВК на ідентифікаторах — для направленого шифрування. Головною перевагою системи, на думку розробників, є відсутність перевірки сертифікату одержувача перед відправкою повідомлення. Механізми взаємодії користувачів з різних доменів та дії у разі компрометації ключів ІВК на ідентифікаторах не уточнюються.

Зазначимо, що у всіх цих системах не вирішується проблема призначення та розповсюдження відкритих ідентифікаторів. Очевидно, що у інформаційній системі, яка налічує мільйони користувачів, практично неможливо розробити політику призначення загальновідомих та відкритих ідентифікаторів.

Ціль – розробка моделі комбінованої ІВК, що має переваги ІВК як на базі X.509, так і на базі ідентифікаторів; розробка методу направленого шифрування, що дозволяє вирішити проблемні питання взаємодії користувачів та узгодження загальносистемних параметрів у такій ІВК.

Задачі: 1) розробка моделі комбінованої інфраструктури відкритих ключів; 2) розробка протоколу узгодження загальносистемних параметрів та взаємодії користувачів.

Об'єкт дослідження – процеси криптографічних перетворень у ІВК при реалізації узгодження загальносистемних параметрів та направленого шифрування.

Предмет дослідження – модель комбінованої ІВК, метод направленого шифрування, що дозволяють налагодити взаємодію користувачів з доменів, які застосовують різні загальносистемні параметри.

Попередні дослідження показують, що створювати ІВК на ідентифікаторах має сенс тільки у рамках деякої організації. Таким чином, будуть існувати багато доменів з різними системними параметрами та політиками безпеки. Серед проблемних питань, які необхідно вирішити для побудови такої системи, є питання взаємодії користувачів різних доменів та узгодження загальносистемних параметрів цих доменів.

1. Архітектура комбінованої ІВК

Сутність розробленої комбінованої інфраструктури відкритих ключів полягає у тому, що уся множина користувачів поділяється на групи (домени). На практиці групою можна вважати деякий відділ, організацію, міністерство тощо. Усі користувачі певної групи використовують ІВК на базі ідентифікаторів. Таким чином, структура групи щонайменше складається з УГК та користувачів. Зазначимо, що УГК кожної групи визначає загальносистемні параметри, політику безпеки та ідентифікатори користувачів, які мають бути цілісними, автентичними та доступними у межах групи. Ідентифікатори користувачів можуть бути представлені у вигляді бази даних.

Можливість перевірки користувачем будь-якої групи цілісності та автентичності бази даних ідентифікаторів, загальносистемних параметрів та політики безпеки довільно фіксованої групи досягається шляхом використання ІВК на базі X.509. Зазначимо, що у роботі архітектура ІВК на базі X.509 не визначається у повному обсязі. Вважається, що використовуються усі необхідні сервіси, які надає традиційна ІВК (OCSP, TSP, реєстрація користувачів тощо).

Особливістю розробленої комбінованої ІВК є наявність серверу підпису, який є елементом групи та забезпечує цілісність, автентичність, доступність та своєчасне поновлення бази даних ідентифікаторів користувачів групи шляхом накладання електронного цифрового підпису (ЕЦП). Сервер підпису використовує пару ключів, що визначена ІВК на базі X.509, тобто сервер підпису має сертифікат відкритого ключа. Цілісність та автентичність загальносистемних параметрів домену і політики безпеки досягається за рахунок додання їх до розширень сертифікату відкритого ключа серверу підпису. Таким чином, будь-який користувач може перевірити цілісність та справжність загальносистемних параметрів та політики безпеки шляхом перевірки ланцюжка сертифікатів. Зауважимо, що користувачі групи не є суб'єктами ІВК на базі X.509, але програмне забезпечення, яке вони використовують, підтримує необхідні алгоритми перевірки ЕЦП.

Схематично модель комбінованої ІВК зображена на рис. 1. На схемі у якості УГК виступає сервер ключів.

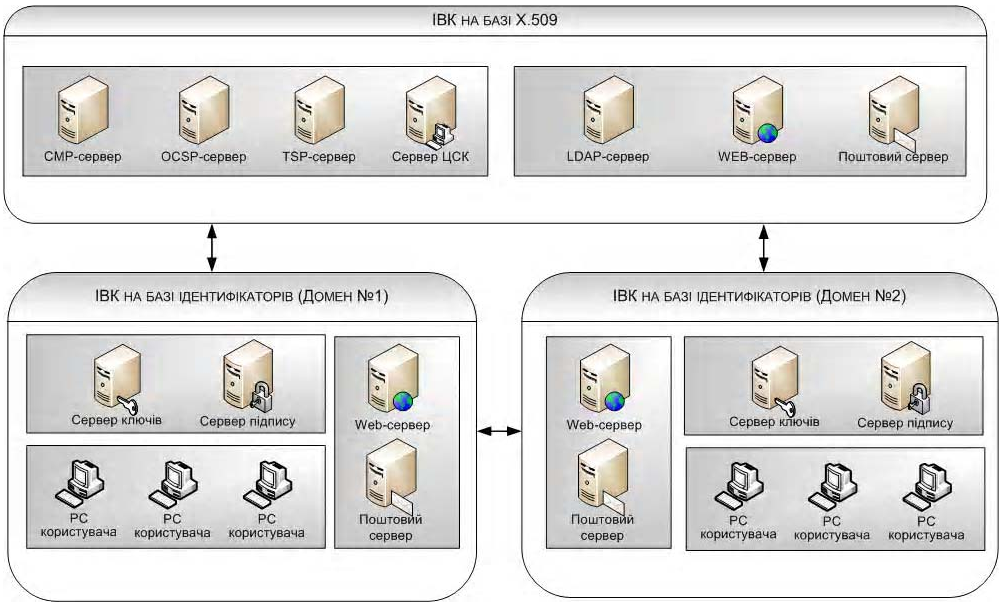

Рис. 1. Архітектура комбінованої інфраструктури відкритих ключів

Розглянемо механізм направленого шифрування (НШ). У випадку належності користувачів одному домену схема направленого шифрування відбувається тільки у межах ІВК на базі ідентифікаторів, наприклад з використанням схеми Boneh-Franklin [10]. Після формування зашифрованого повідомлення користувач відправляє його іншому користувачу через поштовий сервер. Одержувач повідомлення отримує особистий ключ з серверу ключів або, у разі наявності ключа, одразу розшифровує повідомлення. У такому випадку поштовий сервер визначає відправника повідомлення для одержувача.

Якщо користувачі належать різним доменам, то відправник направлено зашифровує повідомлення та підписує його, використовуючи алгоритми НШ, що визначені у зовнішній ІВК на ідентифікаторах, та ЕЦП, що визначені у внутрішній ІВК на ідентифікаторах відповідно. Далі сервер підпису отримує підписане та зашифроване повідомлення, перевіряє ЕЦП, тобто переконується, що зашифроване повідомлення цілісне та дійсно належить користувачу групи. У разі успішної перевірки сервер підпису видаляє ЕЦП користувача, підписує тільки зашифроване повідомлення та відправляє його одержувачу. Зазначимо, що сервер підпису не спроможний розшифрувати повідомлення відправника. Наступним кроком поштовий сервер у групі одержувача самостійно або за допомогою серверу підпису перевіряє ЕЦП та у разі успіху відправляє одержувачу. Одержувач повідомлення отримує особистий ключ з серверу ключів, або у разі наявності ключа одразу розшифровує повідомлення.

Слід відзначити, що схема НШ є досить повільною для великих обсягів даних, тому доцільно використовувати алгоритм симетричного шифрування. Наприклад, відправник генерує ключ та зашифровує повідомлення відповідно до ГОСТ 28147[11], а наступним кроком направлено зашифровує згенерований ключ з використанням схеми Boneh-Franklin [10].

2. Протоколи взаємодії користувачів комбінованої ІВК

Розглянемо формалізовану модель комбінованої інфраструктури ІВК. Нехай задана множина доменів $\Omega = \{\Omega_i \mid i = 1..m\}$, де $m > 0$ - кількість доменів. Вважатимемо, що домен Ω_i складається з серверу генерації ключів S^i_{KG}, серверу підписів S^i_{DS} та множини користувачів $U_i = \{u_{ij} \mid j = 1..n_i\}$, тобто $\Omega_i = \{S^i_{KG}, S^i_{DS}, U_i\}$.

Позначимо центр сертифікації ключів (ЦСК) у ІВК на базі X.509 як S_{PKI}.

Визначимо протокол $\Sigma = \{I, R, U, V\}$ взаємодії користувачів у комбінованій інфраструктурі ключів, як протокол, що складається з чотирьох етапів:

- Етап ініціалізації I.
- Етап генерації ключів користувачів R.
- Етап направленого шифрування U.
- Етап розшифрування V.

Розглянемо **етап ініціалізації,** що складається з встановлення системних параметрів S_{PKI} та з встановлення системних параметрів доменів Ω_i.

Етап встановлення системних параметрів S_{PKI}. Обирається просте число q, група G та генератор групи P порядку q. Центр сертифікації ключів генерує майстер-ключ $d \in [1, q-1]$ та обчислює відкритий ключ $Q = dP$. Позначимо множину загальносистемних параметрів як $D = \{q, G, P\}$. Зазначимо, що відритий ключ Q та множина загальносистемних параметрів D визначені в сертифікаті відкритого ключа S_{PKI}.

Етап встановлення системних параметрів Ω_i. S^i_{DS} генерує особистий ключ $d^i_{DS} \in [1, q-1]$ та обчислює відкритий ключ $Q^i_{DS} = d^i_{DS} P$. Далі вибирається просте число q_i, дві групи $G_1{}^i, G_2{}^i$ порядку q_i та білінійне відображення Вейля або Тейта $e_i : G_1{}^i \times G_1{}^i \to G_2{}^i$ та генератор групи $P_i \in G_1{}^i$. S^i_{KG} генерує майстер-ключ $d^i_{KG} \in Z^*_{q_i}$ та обчислює відкритий ключ $Q^i_{KG} = d^i_{KG} P_i$. Далі обираються криптографічні геш-функції $H^i_1 : \{0,1\}^* \to G^i_1$ та $H^i_2 : G^i_2 \to \{0,1\}^l$ для деякого l. Таким чином, d^i_{DS}, Q^i_{DS} – це пара ключів традиційної ІВК, а d^i_{KG}, Q^i_{KG} – пара ключів ІВК на базі ідентифікаторів. Системними параметрами домену Ω_i будуть $D_i = \{q_i, G^i_1, G^i_2, \hat{e}_i, P_i, H^i_1, H^i_2\}$. Відритий ключ Q^i_{DS} та множина загальносистемних параметрів D_i визначені в сертифікаті відкритого ключа S^i_{DS}. Позначимо базу ідентифікаторів користувачів домену Ω_i як $DB_i = \{ID_{ij} \mid j = 1..n_i\}$. База даних DB_i підписується на ключі d^i_{DS}.

Етап генерації ключів користувачів визначається так:

Кожному користувачу u_{ij} домену Ω_i відповідає ідентифікатор $ID_{ij} \in \{0,1\}^*$. Будь-якому ідентифікатору $ID_{ij} \in \{0,1\}^*$ однозначно відповідає відкритий ключ $Q_{ij} = H_1^i(ID_{ij}) \in G_1{}^i$ та таємний ключ $d_{ij} = d_{KG}^i Q_{ij}$, що формується по запиту користувача до S_{KG}^i.

Процес встановлення ключових даних має такий вигляд (рис. 2).

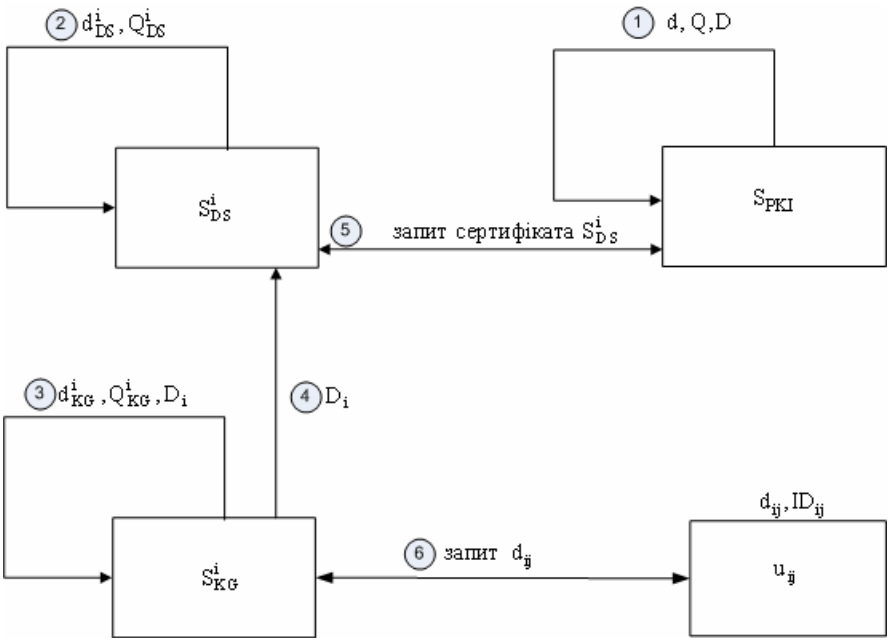

Рис. 2. Схема розподілення ключових даних

Наступним кроком визначимо протоколи направленого шифрування та розшифрування у межах різних доменів (рис. 3) або одного і того ж домену (рис. 4). Зафіксуємо домени Ω_i та Ω_r. Оберемо двох користувачів $u_{ij} \in \Omega_i$ та $u_{rs} \in \Omega_r$ і розглянемо два випадки $i = r$ (один домен) та $i \neq r$ (різні домени).

Визначимо **етап направленого шифрування**.

У випадку $i \neq r$ протокол направленого шифрування користувача u_{ij} на користувача u_{rs} описується так:

1. Користувач u_{ij} звертається до веб-серверу домену Ω_r та отримує сертифікат відкритого ключа серверу підпису S_{DS}^r та базу DB_r. Наступним кроком користувач u_{ij} перевіряє справжність сертифікату, перевіряючи підпис S_{PKI} за допомогою відкритого ключа Q, та отримує з нього загальносистемні параметри D_r. Далі користувач u_{ij} перевіряє цілісність бази даних шляхом перевірки цифрового підпису на відкритому ключі Q_{DS}^r та отримує відкритий ідентифікатор ID_{rs} користувача u_{rs}.

2. Користувач u_{ij} направлено зашифровує повідомлення M, використовуючи відкритий ключ Q_{rs} та загальносистемні параметри D_r, а потім підписує його на своєму особистому ключі d_{ij}. У результаті отримується зашифроване та підписане повідомлення $S_{d_{ij}}(E_{Q_{rs}}(M))$, яке він надсилає на сервер цифрового підпису S_{DS}^i.

3. Сервер S_{DS}^i перевіряє підпис користувача u_{ij} та у разі успіху підписує зашифроване повідомлення $E_{Q_{rs}}(M)$ на особистому ключі d_i. Отримане повідомлення $S_{d_i}(E_{Q_{rs}}(M))$ надсилається на поштовий сервер домену Ω_r.

Аналогічним чином визначимо **етап розшифрування** для випадку $i \neq r$.

1. Поштовий сервер домену Ω_r звертається до веб-серверу домену Ω_i, та отримує сертифікат серверу S^i_{DS}. Наступним кроком поштовий сервер домену Ω_r перевіряє справжність сертифікату. Поштовий сервер домену Ω_r перевіряє цілісність повідомлення шляхом перевірки цифрового підпису на відкритому ключі Q^i_{DS}. У разі успіху поштовий сервер домену Ω_r надсилає повідомлення користувачу u_{rs}.

2. Користувач u_{rs}, у разі відсутності у нього особистого ключа, звертається до сервера ключів S^r_{KG} з запитом на отримання ключа.

3. Сервер ключів генерує d_{rs} та надсилає його користувачу u_{rs}.

4. Користувач u_{rs} розшифровує повідомлення M за допомогою ключа d_{rs}.

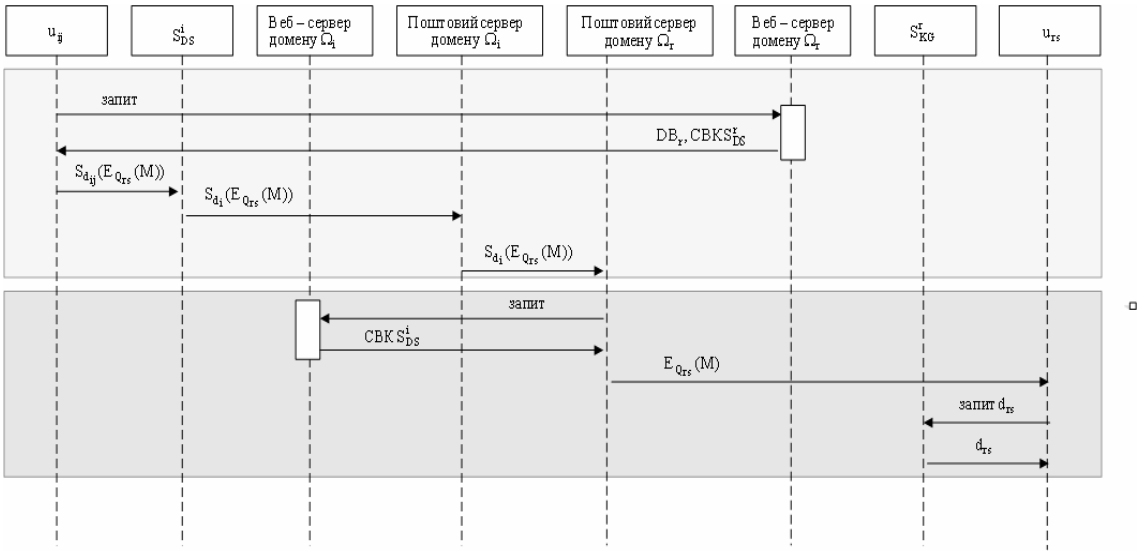

Рис. 3. Протокол взаємодії користувачів

У випадку $i = r$ **етап направленого шифрування** користувача u_{ij} на користувача u_{is} має вигляд.

1. Користувач u_{ij} звертається до веб-серверу домену Ω_i та отримує сертифікат відкритого ключа серверу підпису S^i_{DS} та базу DB_i. Наступним кроком користувач u_{ij} перевіряє справжність сертифікату, перевіряючи підпис S_{PKI} за допомогою відкритого ключа Q, та отримує з нього загальносистемні параметри D_i. Далі користувач u_{ij} перевіряє цілісність бази даних шляхом перевірки цифрового підпису на відкритому ключі Q^i_{DS} та отримує відкритий ідентифікатор ID_{is} користувача u_{is}.

2. Користувач u_{ij} направлено зашифровує повідомлення M, використовуючи відкритий ключ Q_{is} та загальносистемні параметри D_i, і надсилає користувачу u_{is} через поштовий сервер домену Ω_i.

Етап розшифрування для випадку $i = r$.

1. Користувач u_{is}, у разі відсутності у нього особистого ключа, звертається до сервера ключів S^i_{KG} з запитом на отримання ключа.

2. Сервер ключів генерує для користувача u_{is} особистий ключ та надсилає його користувачу u_{is}.

3. Користувач u_{is} розшифровує повідомлення M за допомогою ключа d_{is}.

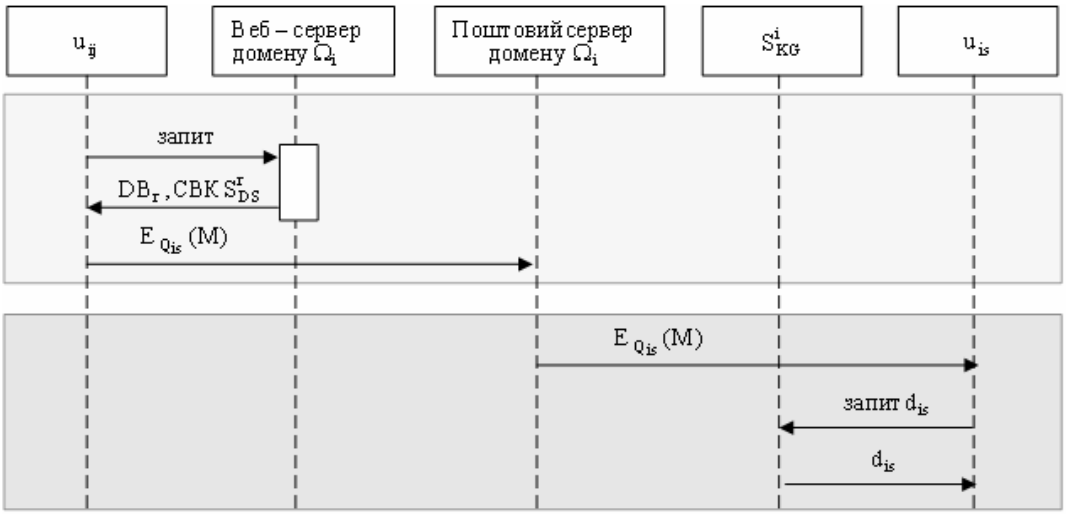

Рис. 4. Протокол взаємодії користувачів

3. Вирішення проблемних питань при розгортанні та використанні комбінованої ІВК

Щоб практично побудувати комбіновану ІВК, яка дозволить знизити вартість послуг безпеки, необхідно вирішити такі питання:

1. Розповсюдження загальносистемних параметрів.
2. Розроблення політики безпеки.

Розглянемо більш детально проблему розповсюдження загальносистемних параметрів. По-перше, зауважимо, що криптографічні примітиви у ІВК на базі X.509 та на базі ідентифікаторів не можуть використовувати однакові загальносистемні параметри. Криптографічні примітиви у ІВК на базі ідентифікаторів на поточний момент базуються на використанні еліптичних кривих, що не задовільняють MOV-умові, у той час як криптографічні примітиви у ІВК на базі X.509 використовують еліптичні криві, що задовільняють зазначеній умові. Що стосується множини доменів, у яких функціонує ІВК на базі ідентифікаторів, то у загальному випадку слід вважати, що для кожного домену задані свої загальносистемні параметри.

Таким чином, постає задача розповсюдження автентичних загальносистемних параметрів з метою унеможливлення атак, що базуються на підміні відкритих параметрів системи. Загальносистемні параметри ІВК на базі X.509 містять в сертифікаті, тобто їх цілісність та справжність гарантується ЦСК, що випустив сертифікат. Щодо загальносистемних параметрів ІВК на базі ідентифікаторів, то дослідниками було запропоновано декілька підходів [4]. Параметри можуть бути включені до сертифікату відкритого ключа як додаткові поля, але у разі компрометації особистого ключа, що відповідає відкритому ключу сертифіката, доведеться перевипускати сертифікат. Альтернативою цьому підходу є використання сертифікату атрибутів для загальносистемних параметрів. Але зважаючи на те, що в Україні не підтримуються сертифікати атрибутів, у запропонованій комбінованій ІВК використовується перший підхід.

Сервер генерації ключів визначає загальносистемні параметри домену та передає їх серверу підпису, який додає їх до свого запиту на сертифікат. Фактично, якщо сервер генерації передав загальносистемні параметри серверу підпису, то він повинен звернутися із запитом до ЦСК на перевипуск сертифікату. Але загальносистемні параметри не змінюються часто, тому це суттєво не вплине на частоту перевипуску сертифікату. У випадку блокування або скасування сертифікату серверу підпису загальносистемні параметри немає потреби змінювати, а необхідно лише додати до нового сертифікату відкритого ключа серверу підпису.

При розробці політики безпеки домену слід вирішити питання формування та розповсюдження ідентифікаторів користувачів домену, а також порядок генерації та видачі особистих ключів користувачів домену.

Відкриті ідентифікатори користувачів повинні бути загальнодоступними та зручними для запам'ятовування строками. Пропонується використовувати внутрішні поштові адреси. Одна із проблем, яку необхідно вирішити, була описана у роботі Callas [5]. Її сутність полягає у тому, що у разі відкритого доступу до усіх ідентифікаторів групи зловмисник може дослідити її структуру або розсилати спам. Щоб запобігти цьому, пропонується використовувати відкриту базу ідентифікаторів (яка містить ідентифікатори публічних співробітників організації) та закриту, до якої мають доступ тільки співробітники.

Проблема захищеного отримання ключа від центру сертифікації є однією з найважливіших для інфраструктури відкритих ключів. Традиційна ІВК вирішує це питання за допомогою отримання таємного ключа безпосередньо у приміщені центру сертифікації. Такий підхід може бути прийнятним у разі довгострокових ключів, якщо ж ключі є короткостроковими, то отримання особистого ключа у приміщені сторонньої організації призводить до значних накладних витрат. У схемі компанії Voltage це питання вирішується шляхом суворої автентифікації користувача на ключовому сервері з використанням сертифікатів. Таким чином, користувач повинен володіти довгостроковим ключем для отримання короткострокового, що суперечить ідеї ІВК на базі ідентифікаторів, згідно з якою користувачі не мають сертифікатів. У запропонованій моделі ключовий сервер розташовується у межах тієї ж групи, що і користувач, тобто витрати часу на отримання особистого ключа будуть значно менші. Також пропонується використовувати неінтерактивний метод. Необхідно зазначити, що на відміну від традиційної ІВК, користувач не повинен отримувати особистий ключ на кожний період, а тільки тоді, коли у цьому є потреба.

Відкриті ключі змінюються автоматично за рахунок конкатенації відкритого ідентифікатора користувача та мітки часу (період зміни якої встановлюється у політиці безпеки відповідної групи).

До переваг розробленої системи можна віднести:

1. Масштабованість системи.
2. Використання ідентифікаторів як відкритих ключів для кінцевих користувачів.
3. Можливість взаємодії користувачів з різних доменів з різними загальносистемними параметрами.
4. Забезпечення конфіденційності, цілісності та справжності.
5. Можливість підключення додаткових сервісів (антивірус, антиспам тощо).
6. Можливість контролю кореспонденції з боку керівництва (якщо є потреба).

Основними недоліками розробленої системи є:

1. Навантаження на сервер підпису домену (слід виконувати формування та перевірку підпису для кожного електронного листа).
2. Необхідність перепідписувати базу ідентифікаторів при реєстрації або видаленні нового користувача.
3. Розробка апаратних модулів, що підтримували б криптографічні примітиви у ІВК на базі ідентифікаторів.

4. Висновки

Наукова новизна представлена новою моделлю комбінованої ІВК, яка поєднує ІВК на базі X.509 та ІВК на базі ідентифікаторів. Особливістю розробленої моделі комбінованої ІВК є наявність відокремленого серверу підпису, який забезпечує цілісність, автентичність, доступність та своєчасне поновлення бази даних ідентифікаторів користувачів домену та загальносистемних параметрів.

Також був розроблений метод направленого шифрування у комбінованій ІВК для взаємодії користувачів з різних доменів, що мають різні загальносистемні параметри та політики безпеки.

Практична значущість полягає у зменшені вартості усієї системи, що обумовлено скороченням кількості сертифікатів завдяки застосуванню ІВК на базі ідентифікаторів на рівні кінцевих користувачів. Практична значимість методу направленого шифрування полягає у можливості взаємодії користувачів доменів з різними загальносистемними параметрами. Сутність методу полягає у формуванні підписаних загальносистемних параметрів, отриманні та перевірці параметрів користувачем іншого домену, направленому шифруванні

повідомлення на отриманих параметрах та перевірці цілісності отриманого зашифрованого повідомлення сервером підпису.

Зазначимо, що основними недоліками системи є навантаження на сервер підпису та необхідність перепідписування бази ідентифікаторів при реєстрації або видаленні нового користувача. Проте домен комбінованої ІВК налічує в середньому не більш ніж 500 користувачів, тому загальне навантаження на сервер підпису не є великим.

У подальшому планується визначити структури розширень сертифікатів, що відносяться до ІВК на базі ідентифікаторів, а також формати підписаних та зашифрованих даних.

Список літератури: **1**. *Горбенко І.Д., Онопрієнко В.В.* Стан та проблемні питання створення та розвитку Національної ІВК //Прикладна радіоелектроніка. 2006. Том.5. №1. С. 41-51 **2.** *ITU-T* (International Telecommunications Union) Recommendation X.509: Information Technology - Open Systems Interconnection The Directory: Authentication Framework. 2000 **3.** *Voltage* Security. Identity-Based Encryption and PKI Making Security Work. 2005. **4.** *Geraint Price, Chris J.* Mitchell: Interoperation Between a Conventional PKI and an ID-Based Infrastructure. EuroPKI 2005: 73-85. **5.** *Girault M.* Self-certified public keys. In D. W. Davies, editor, Advances in Cryptology — EUROCRYPT'91, volume 547 of Lecture Notes in Computer Science. 1992. P. 490–497. Springer-Verlag. **6**. *Gentry C.* Certificate-based encryption and the certificate revocation problem. In E. Biham, editor, Advances in Cryptology – EUROCRYPT 2003, volume 2656 of Lecture Notes in Computer Science, pages 272–293. Springer-Verlag, 2003. **7**. *Al-Riyami S., Paterson K. G.* Certificateless Public Key Cryptography, extended abstract in Proceedings of ASIACRYPT '03, LNCS 2894, Springer-Verlag, 2003. **8.** *Chen L., Harrison K., Moss A., Soldera D., and Smart N.P.* Certification of public keys within an identity based system. In A. H. Chan and V. D. Gligor, editors, Information Security, 5th International Conference, ISC, volume 2433 of LNCS, pages 322–333. Springer-Verlag, 2002. **9**. *Callas J.* Identity-Based Encryption with Conventional Public-Key Infrastructure. In 4th Annual PKI R&D Workshop, number 7224 in Interagency Reports, pages 102–115. NIST, 2005. **10**. *Boneh D. and Franklin M.* Identity-based encryption from the Weil pairing. Advances in Cryptology - CRYPTO 2001, volume 2139 of Lecture Notes in Computer Science. Springer-Verlag. 2001.P. 213-229. **11.** *ГОСТ* 28147-89 "Государственный стандарт Союза ССР. Система обработки информации. Защита криптографическая. Алгоритм криптографического преобразования".

Поступила в редколлегию 01.06.2011

Погребняк Костянтин Анатолійович, канд. техн. наук, доцент каф. БІТ ХНУРЕ. Адреса: Україна, 61166, Харків, пр. Леніна, 14, e-mail: iitkostya@gmail.com

Кравченко Павло Олександрович, аспірант каф. БІТ ХНУРЕ. Адреса: Україна, 61166, Харків, пр. Леніна, 14, e-mail: kravchenkopo@gmail.com