МІНІСТЕРСТВО ОСВІТИ І НАУКИ, МОЛОДІ ТА СПОРТУ УКРАЇНИ

ХАРКІВСЬКИЙ НАЦІОНАЛЬНИЙ УНІВЕРСИТЕТ РАДІОЕЛЕКТРОНІКИ

КРАВЧЕНКО ПАВЛО ОЛЕКСАНДРОВИЧ

УДК 681.3.06 : 519.248.681

МОДЕЛЬ ТА МЕТОДИ ЗАБЕЗПЕЧЕННЯ ПОСЛУГ БЕЗПЕКИ У КОМБІНОВАНИХ ІНФРАСТРУКТУРАХ ВІДКРИТИХ КЛЮЧІВ

05.13.05 – комп`ютерні системи та компоненти

АВТОРЕФЕРАТ

дисертації на здобуття наукового ступеня

кандидата технічних наук

Харків – 2012

Дисертацією є рукопис.

Робота виконана у Харківському національному університеті радіоелектроніки Міністерства освіти і науки, молоді та спорту України.

Науковий керівник: доктор технічних наук, професор
Бондаренко Михайло Федорович, Харківський національний університет радіоелектроніки, ректор.

Офіційні опоненти: доктор технічних наук, професор
Краснобаєв Віктор Анатолійович, Полтавський національний технічний університет ім. Ю. Кондратюка, завідувач кафедри комп'ютерної інженерії;

кандидат технічних наук, доцент
Єсін Віталій Іванович, Харківський національний університет ім. В.Н. Каразіна, доцент кафедри безпеки інформаційних систем і технологій.

Захист відбудеться « » _____ 2012 р. о ___ годині на засіданні спеціалізованої вченої ради К 64.052.01 у Харківському національному університеті радіоелектроніки за адресою: 61166, м. Харків, просп. Леніна, 14.

З дисертацією можна ознайомитися у бібліотеці Харківського національного університету радіоелектроніки за адресою: 61166, м. Харків, просп. Леніна, 14.

Автореферат розісланий «__» _____ 2012 р.

Вчений секретар
спеціалізованої вченої ради Є. І. Литвинова

ЗАГАЛЬНА ХАРАКТЕРИСТИКА РОБОТИ

Актуальність теми. Для забезпечення якісного надання послуг конфіденційність, цілісніть та доступність в інформаційно-телекомунікаційних системах створені та використовуються інфраструктури відкритих ключів (ІВК). Основне розповсюдження отримали ІВК, що базуються на виготовленні та обслуговуванні сертифікатів відкритих ключів, у яких використовуються ЕЦП та направлене шифрування. Незважаючи на те, що такі системи отримали широке розповсюдження, вони мають суттєві недоліки, перш за все, значну вартість та складність обслуговування сертифікатів, психологічну неприйнятність тощо. На етапі розроблення та використання знаходяться ІВК, що базуються на ідентифікаторах користувачів та математичному апараті спарювання точок еліптичних кривих, та дозволяють відмовитися від сертифікатів відкритих ключів користувачів, і як результат – скоротити загальну вартість володіння системою до трьох разів. На сьогодні у розробці знаходяться стандарти IEEE P1363.3/D1-2008, RFC 5091- 2007, RFC 5408-2009, що описують протоколи та криптопримітиви у ІВК на ідентифікаторах. Але в явному вигляді і такі ІВК мають недоліки, що пов’язані з високим необхідним рівнем довіри до уповноваженого на генерацію ключів, відсутністю механізмів забезпечення цілісності та справжності загальносистемних параметрів та ідентифікаторів користувачів, наявністю конфіденційного каналу зв’язку між користувачем та уповноваженим на генерацію ключів. Одним з найбільш перспеспективних напрямків розвитку є комбіновані ІВК, у яких на рівні організацій застосовуються системи ІВК з сертифікатами, а на рівні користувачів – ІВК на базі ідентифікаторів, що дозволяє досягти компромісу між вартістю системи та рівнем захисту.

Проте, створення комбінованої ІВК має проблемні питання та протиріччя, які полягають у відсутності механізмів забезпечення цілісності загальносистемних параметрів та ідентифікаторів користувачів ІВК на базі ідентифікаторів, ефективних методів направленого шифрування для користувачів, що не володіють погодженими загальносистемними параметрами.

Таким чином, актуальною науково-технічною задачею є розробка моделі та методів забезпечення послуг безпеки у комбінованій інфраструктурі відкритих ключів.

Зв'язок роботи з науковими програмами, планами, темами. Дисертаційна робота виконана в рамках держбюджетної НДР № 262-1 від 01.01.2011 р. «Розвиток, стандартизація, уніфікація, удосконалення та впровадження інфраструктури відкритих ключів, включаючи національну систему ЕЦП на національному та міжнародному рівнях» (за наказом МОНУ №1177 від 30.11.2010 р.); госпдоговірної НДР № 09-06 від 22 січня 2009 р. "Дослідження та розробка комбінованих інфраструктур з відкритими ключами на основі використання існуючих ІВК та системи на ідентифікаторах"

(ДР № 0109U002498); госпдоговірної НДР № 11-06 від 01.03.2011р. "Розробка методів, комплексів та засобів інфраструктури відкритих ключів (ІВК) для національних та міжнародних інформаційно-телекомунікаційних систем та інформаційних технологій" (ДР № 0111U002634); НДР № 07-65 "Дослідження методів та протоколів автентифікації у системах захисту від несанкціонованого доступу" (ДР № 0108U000036).

Мета дослідження – розробка моделі та методів забезпечення послуг безпеки у комбінованій інфраструктурі відкритих ключів за рахунок використання унікальних загальносистемних параметрів та політик безпеки для множин користувачів, що дозволяє реалізувати модель взаємної недовіри та взаємного захисту.

Для досягнення поставленої мети необхідно вирішити такі завдання:

– розробити модель комбінованої ІВК, що забезпечує цілісність загальносистемних параметрів та ідентифікаторів користувачів;

– розробити метод направленого шифрування для користувачів, що не володіють погодженими загальносистемними параметрами;

– розробити метод генерації ключів для комбінованої ІВК, що дозволить збільшити показники доступності розподіленого уповноваженого на генерацію ключів;

– дослідити методи автоматичного аналізу безпеки криптографічних протоколів;

– розробити програмний макет ІВК на базі ідентифікаторів для дослідження процесів генерації ключів, направленого шифрування та електронного цифрового підпису.

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

Предмет дослідження – модель та методи забезпечення послуг безпеки у комбінованих ІВК.

Методи дослідження – методи теорії чисел – під час розробки моделі та методів комбінованої ІВК, аналіз і синтез комбінованої ІВК, методи теорії ймовірностей при визначенні криптографічної стійкості перетворень типу НШ та показників доступності розподіленого уповноваженого на генерацію ключів, методи практичної криптографії та системного аналізу при порівнянні існуючих комбінованих ІВК, методи програмного моделювання при реалізації процесів криптографічних перетворень тощо.

Наукова новизна одержаних результатів

1. Вперше отримано модель комбінованої ІВК, яка характеризується використанням унікальних загальносистемних параметрів та політик безпеки ІВК на базі ідентифікаторів для різних множин користувачів, забезпеченням цілісності ідентифікаторів і загальносистемних параметрів, що дозволяє реалізувати модель взаємної недовіри і взаємного захисту.

2. Удосконалено метод направленого шифрування у комбінованій ІВК, який відрізняється від існуючих протоколами отримання і перевірки загальносистемних параметрів та ідентифікатора отримувача і дозволяє взаємодіяти користувачам, які не володіють погодженими загальносистемними параметрами, що дозволяє скоротити кількість необхідних операцій шифрування у 3 рази порівняно з прототипом.

3. Удосконалено метод генерації особистого ключа для комбінованої ІВК, який відрізняється паралельними запитами користувача до розподіленого уповноваженого на генерацію ключів та формуванням особистого ключа користувачем, що дозволяє збільшити показники доступності для розподіленого уповноваженого на генерацію ключів.

4. Удосконалено метод аналізу безпеки криптопротоколів, який відрізняється від існуючого пошуком збігів термів у попередніх сеансах протоколу та сеансах протоколу з іншими учасниками, що дозволяє знайти протоколи, які не є криптоживучими.

Практичне значення одержаних результатів

1. Запропонована модель комбінованої інфраструктури відкритих ключів є науково-методичною основою для практичного створення комбінованих ІВК, та вирішує практичне питання забезпечення цілісності загальносистемних параметрів та ідентифікаторів користувачів і їх розповсюдження.

2. На основі розроблених у дисертації методів синтезовано протокол направленого шифрування і протокол генерації та видачі ключів.

3. Реалізований програмний макет інфраструктури відкритих ключів на базі ідентифікаторів дозволяє дослідити процеси генерації ключів, направленого шифрування та електронного цифрового підпису.

4. Отримані аналітичні вирази можуть бути використані під час розрахунку вартості розподіленого уповноваженого на генерацію ключів.

Результати дисертаційної роботи впроваджено у ЗАТ «Інститут інформаційних технологій» (акт від 12.10.2011 р.); у Харківському національному університеті радіоелектроніки в навчальному процесі у дисциплінах «Прикладна криптологія» та «Криптографічні системи та протоколи» (акт від 14.10.2011 р.).

Особистий внесок здобувача. Усі основні положення та результати роботи автор отримав особисто. У публікаціях, опублікованих у співавторстві, здобувачеві належать: [3] – аналіз існуючих методів генерації та видачі ключів, [4] – аналіз існуючих досліджень галузі побудови комбінованої ІВК, [6] – модель комбінованої ІВК, [7] – метод направленого шифрування та доведення його стійкості у моделі випадкового оракула, [8] – аналіз нормативних документів у галузі побудови ІВК на базі ідентифікаторів, [9] – удосконалений метод аналізу безпеки криптографічних протоколів, [11] – модель комбінованої ІВК та удосконалений метод направленого шифрування, [18] – удосконалений метод генерації та видачі ключів для розподіленого уповноваженого на генерацію ключів.

Апробація результатів дисертації. Основні положення та результати дисертаційної роботи представлено та обговорено на дев'яти конференціях: 1) Конференція "Наукові доробки молоді – вирішенню проблем європейської інтеграції" 20-21 березня 2007 р. (м. Харків); 2) 12-й міжнародний молодіжний форум "Радиоэлектроника и молодежь в XXI веке", 1-3 квітня 2008 р. (м. Харків); 3) XI Міжнародна науково-практична конференція "Безопасность информации в информационно-телекоммуникационных системах", 20 – 23 травня 2008 р. (м. Київ); 4) 4 міжнародна науково-технічна конференція "Гаранто-способные (надежные и безопасные) системы, сервисы и технологии", 22 – 25 квітня 2009 р. (м. Кіровоград); 5) XII Міжнародна науково-практична конференція "Безопасность информации в информационно-телекоммуникационных системах", 19 – 22 травня 2009 р. (г. Київ); 6) X Міжнародна конференція "Сучасні проблеми радіоелектроніки, телекомунікацій та комп'ютерної інженерії", 23 – 27 лютого 2010 р. (м. Львів-Славське); 7) 5 міжнародна науково-технічна конференція "Гаранто-способные (надежные и безопасные) системы, сервисы и технологии", 11 – 15 травня 2010 р. (м. Кіровоград); 8) XIII Міжнародна науково-практична конференція "Безопасность информации в информационно-телекоммуникационных системах", 18 – 21 травня 2010 р. (м. Київ); 9) 1st international workshop "Critical infrastructure safety and security", 11 – 13 May, 2011 (м. Кіровоград).

Публікації. Основні положення й результати дисертаційної роботи опубліковано у 19 друкованих працях, серед яких 1 монографія, 9 статей у наукових журналах та 2 статті у збірниках наукових праць, які входять до переліку наукових фахових видань України, 7 тез доповідей у збірниках науково-технічних міжнародних конференцій.

Структура та обсяг дисертації. Дисертація містить 107 сторінок основного тексту, 22 рисунка. Її структура складається з вступу, пяти розділів, 30 підрозділів, висновків, списку використаних джерел з 82 назв на 9 сторінках та одного додатка (на 4 с.).

ОСНОВНИЙ ЗМІСТ РОБОТИ

Вступ містить обгрунтування актуальності задачі, що розв'язується, формулювання мети, предмета, об'єкта та задач дослідження, сукупність наукових результатів, що виносяться на захист, відомості про їх апробацію та реалізацію, а також характеристику особистого внеску здобувача.

У першому розділі дисертації наведено порівняльний аналіз сучасних комбінованих інфраструктур відкритих ключів, їх характеристик, переваг та недоліків, сформульовано критерії порівняння комбінованих інфраструктур відркритих ключів. Обгрунтовано доцільність використання комбінованих ІВК в умовах жорстких вимог до загальної вартості володіння та застосування унікальних загальносистемних параметрів та політик безпеки для державних та комерційних організацій. Сформульовано мету і задачі дослідження.

Результати проведених досліджень показали, що одним з головних завдань при побудові комбінованої ІВК є застосування унікальних загальносистемних параметрів та політик призначення ідентифікаторів для кожної організації, забезпечення їх цілісності при розповсюдженні та можливість захищеної взаємодії користувачів, що не володіють погодженими загальносистемними параметрами.

Другий розділ дисертації присвячено розробці моделі комбінованої інфраструктури відкритих ключів, що забезпечує цілісність ідентифікаторів і загальносистемних параметрів, що дозволяє реалізувати модель взаємної недовіри і взаємного захисту.

Запропоновано комбіновану ІВК, яка характеризується використанням унікальних загальносистемних параметрів та політик безпеки ІВК на базі ідентифікаторів для різних множин користувачів, архітектура якої наведена на рис. 1.

Множина доменів, кожен з яких застосовує ІВК на базі ідентифікаторів, визначається як $\Omega = \{\Omega_i \,|\, i = 1..m\}$, де $m > 0-$ кількість доменів. Кожен домен Ω_i складається із серверу генерації ключів S^i_{KG}, серверу підписів S^i_{DS} та множини користувачів $U_i = \{u_{ij} \,|\, j = 1..n_i\}$, тобто $\Omega_i = \{S^i_{KG}, S^i_{DS}, U_i\}$.

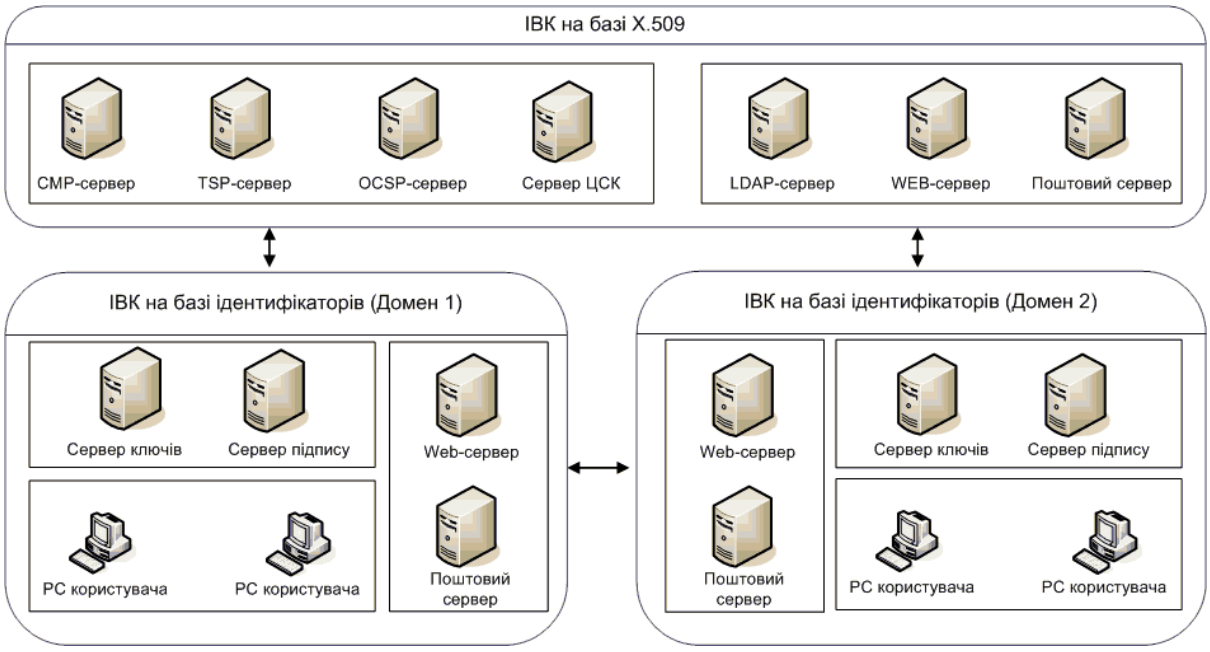

Рис. 1. Архітектура комбінованої ІВК

До параметрів домену Ω_i відносять: просте число q_i, групи G_1^i, G_2^i порядку q_i, білінійне відображення $e_i : G_1^i \times G_1^i \to G_2^i$, генератор групи $P_i \in G_1^i$, особистий ключ $d^i_{DS} \in [1, q-1]$, відкритий ключ $Q^i_{DS} = d^i_{DS} P$, майстер-ключ $d^i_{KG} \in Z^*_{q_i}$, відкритий ключ $Q^i_{KG} = d^i_{KG} P_i$, криптографічні геш-функції

$H_1^i : \{0,1\}^* \to G_1^i$ та $H_2^i : G_2^i \to \{0,1\}^l$ для деякого l. Таким чином, d_{DS}^i, Q_{DS}^i – це пара ключів традиційної ІВК, а d_{KG}^i, Q_{KG}^i – пара ключів ІВК на базі ідентифікаторів. Системними параметрами домену Ω_i будуть $D_i = \{q_i, G_1^i, G_2^i, \hat{e}_i, P_i, H_1^i, H_2^i\}$. Відкритий ключ Q_{DS}^i та множина загальносистемних параметрів D_i визначені у сертифікаті відкритого ключа S_{DS}^i.

Таким чином, сервер ключів S_{KG}^i відповідає за вироблення ключових даних, а сервер підпису використовується для забезпечення цілісності і справжності загальновідомих параметрів домену Ω_i та бази ідентифікаторів $DB_i = \{ID_{ij} \mid j = 1..n_i\}$, що підписується на ключі d_{DS}^i.

За рахунок використання додаткового рівня ієрархії досягається можливість використання унікальних загальносистемних параметрів та політик безпеки для різних організацій, що є однією з умов побудови моделі взаємної недовіри та взаємного захисту. За рахунок введення серверу підпису досягається цілісність загальносистемних параметрів домену та ідентифікаторів користувачів.

Третій розділ дисертації присвячено удосконаленню методу направленого шифрування у комбінованій ІВК для користувачів, що не володіють погодженими загальносистемними параметрами (для різних доменів). Найпростішим рішенням є використання методу Боне-Франкліна, але у цьому разі неможливо реалізувати наскрізне шифрування і доводиться двічі додатково зашифровувати повідомлення для кожної операції направленого шифрування на серверах взаємодії.

Удосконалений метод вирішує це протиріччя за рахунок отримання цілісних загальносистемних параметрів та ідентифікаторів іншого домену користувачем (рис. 2).

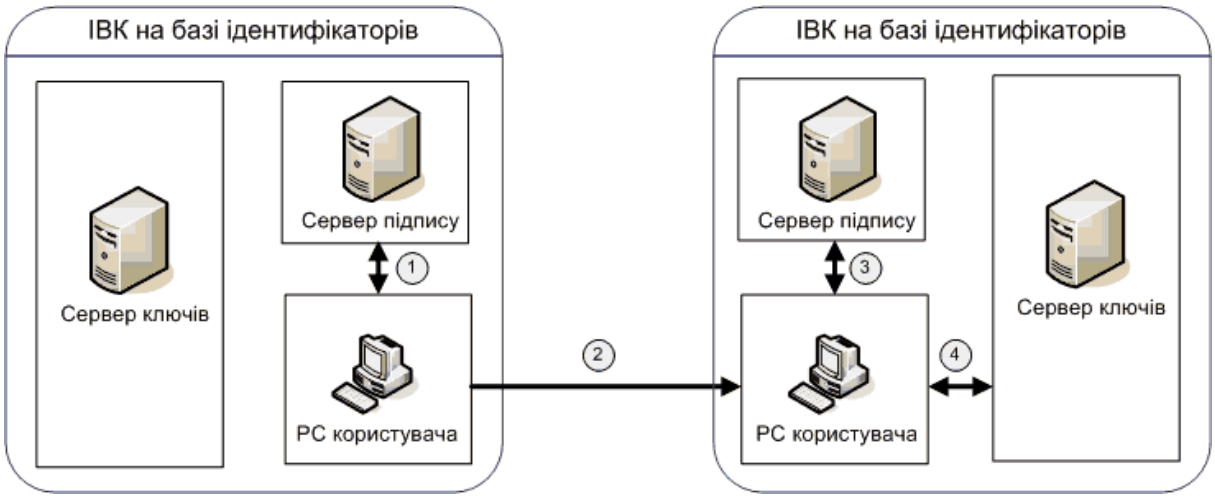

Рис. 2. Схема удосконаленого методу направленого шифрування

Метод $\Sigma = \{I, R, U, V\}$ направленого шифрування у комбінованій інфраструктурі ключів реалізується на таких етапах:

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

Етап ініціалізації складається з встановлення системних параметрів S_{PKI} та з встановлення системних параметрів доменів Ω_i.

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 особистий ключ $d_{ij} = d_{KG}^i Q_{ij}$, що формується за запитом користувача до S_{KG}^i.

Процес встановлення ключових даних має такий вигляд (рис. 3).

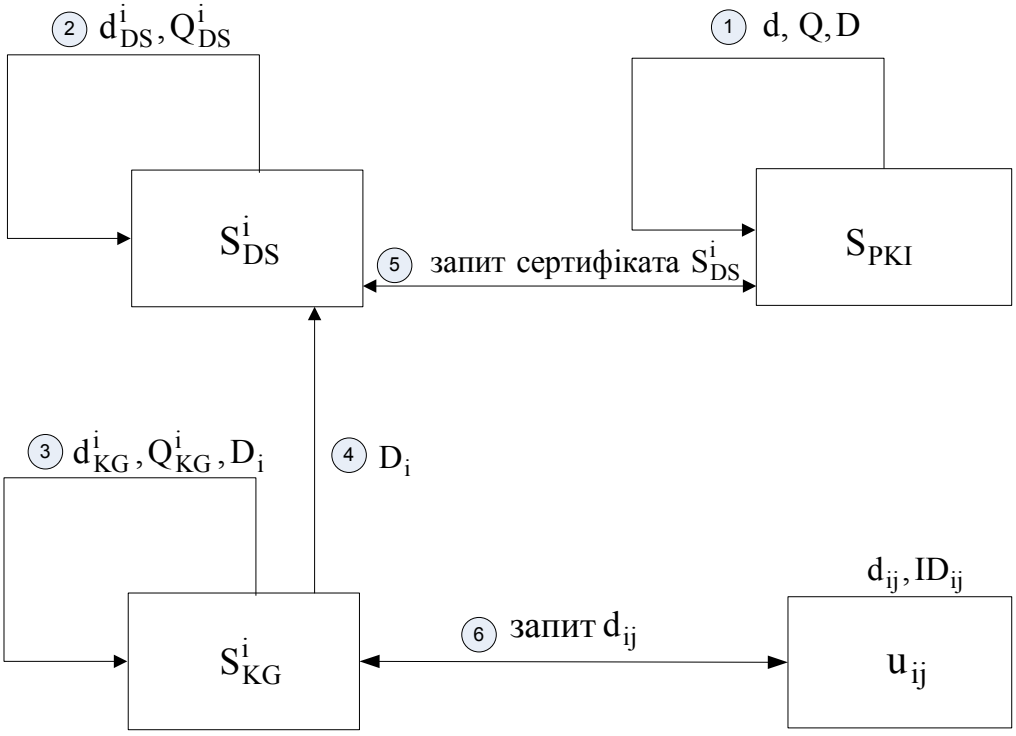

Рис. 3. Схема розподілення ключових даних

Визначено протоколи направленого шифрування та розшифрування для різних доменів (рис. 4). Фіксуються домени Ω_i та Ω_r. На прикладі двох користувачів $u_{ij} \in \Omega_i$ та $u_{rs} \in \Omega_r$ розглянемо протокол направленого шифрування для $i \neq r$ (різні домени).

Визначимо етап направленого зашифрування.

1. Користувач u_{ij} звертається до веб-серверу домену Ω_r та отримує сертифікат відкритого ключа серверу підпису S^r_{DS} та базу DB_r. Наступним кроком користувач u_{ij} перевіряє справжність сертифіката, 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^r_{DS} 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^i_{DS}.

3. Сервер S^i_{DS} 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 визначається 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 сертифіката. 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 серверу ключів S^r_{KG} із 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}.

У моделі випадкового оракула доведено таке твердження:

Твердження. Припустимо, що геш-функції H_1, H_2 є випадковими оракулами. Тоді IDComby є сематнично стійкою схемою шифрування на ідентифікаторах (IND-ID-CPA), якщо BDH є субекспоненційно складною в групах, що генеруються G. Позначимо A як IND-ID-CPA атакуючого, що має перевагу $\varepsilon(k)$ проти схеми IDComby. Припустимо, що A робить якнайбільше $q_E > 0$ запитів на отримання особистого ключа, та $q_{H_2} > 0$ запитів до H_2. Тоді існує

алгоритм B, що вирішує BDH у групі, що генерується G з перевагою якнайменше $Adv_{G,B}(k) \geq \frac{2\varepsilon(k)}{e(1+q_E)\cdot q_{H_2}}$.

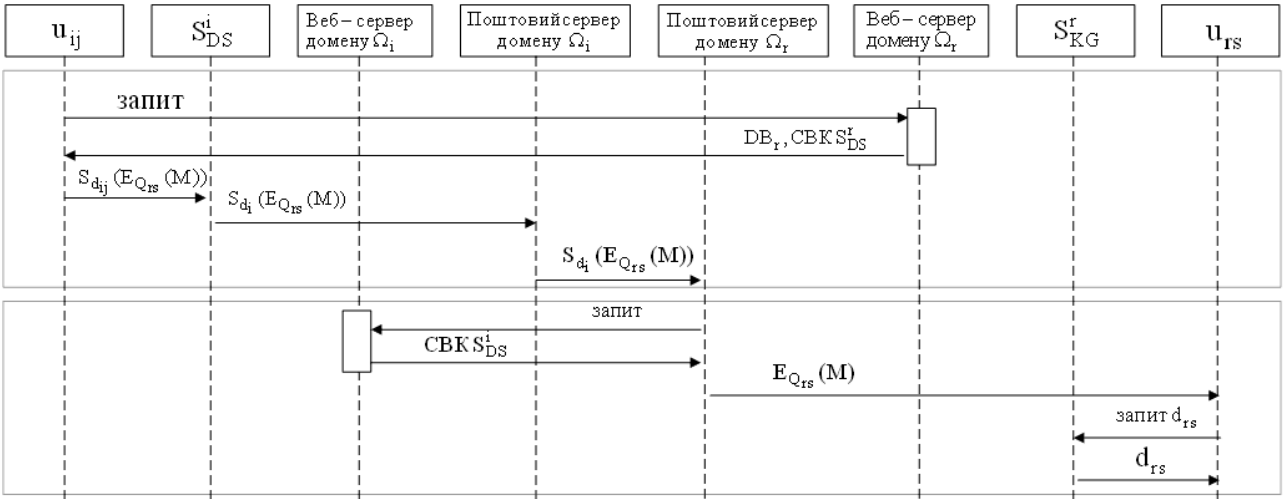

Рис. 4. Метод направленого шифрування

Сутність розробленого у дисертації методу направленого шифрування для користувачів, що не володіють погодженими загальносистемними параметрами, 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.

У четвертому розділі удосконалено метод генерації особистого ключа для комбінованої ІВК, який відрізняється паралельними запитами користувача до розподіленого уповноваженого на генерацію ключів та формуванням особистого ключа користувачем, що дозволяє збільшити показники доступності для розподіленого уповноваженого на генерацію ключів.

Одним з важливих проблемних питань, що потребує рішення, є низька криптоживучість уповноваженого на генерацію ключів у комбінованій ІВК. Це пояснюється тим, що при компрометації майстер-ключа зловмисник може обчислити усі особисті ключі користувачів. Для вирішення цього проблемного питання застосовують криптоживучі ІВК на ідентифікаторах, що характеризуються розподіленим уповноваженим на генерацію ключів (УГК). Майстер-ключ розподіляється між декількома серверами за певним алгоритмом, що дозволяє відновити його тільки у разі участі необхідної кількості серверів.

Для генерації особистого ключа користувача у криптоживучій комбінованій інфраструктурі відкритих ключів застосовують методи генерації та видачі ключів. Наведемо вимоги, яким мають відповідати протоколи, що є реалізацією таких методів:

– неможливість імітації користувачів з боку УГК;

– неможливість обчислення особистого ключа меншою, ніж порогова, кількістю серверів;

– відсутність конфіденційного каналу зв’язку для передавання особистого ключа;

– забезпечення доступності розподіленого уповноваженого на генерацію ключів.

Недоліками відомих методів генерації ключів є те, що у разі виведення з ладу хоча б одного сервера уся система перестане функціонувати. Це є наслідком генерації ключа користувача усіма серверами (рис. 5).

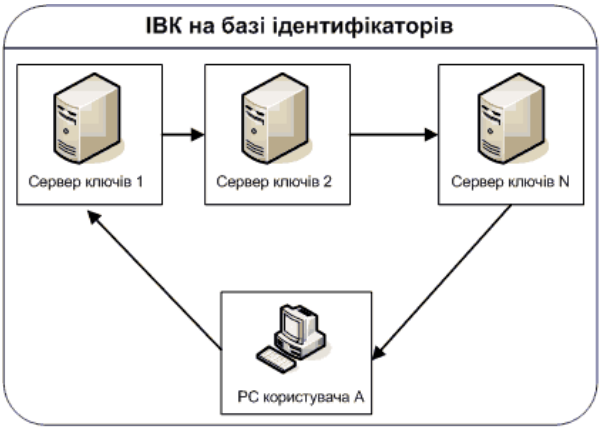

Рис. 5. Схема відомих методів генерації ключів

Удосконалений метод генерації ключів відрізняється від існучих паралельними запитами до уповноважених на генерацію ключів та формуванням особистого ключа користувачем самостійно (рис. 6).

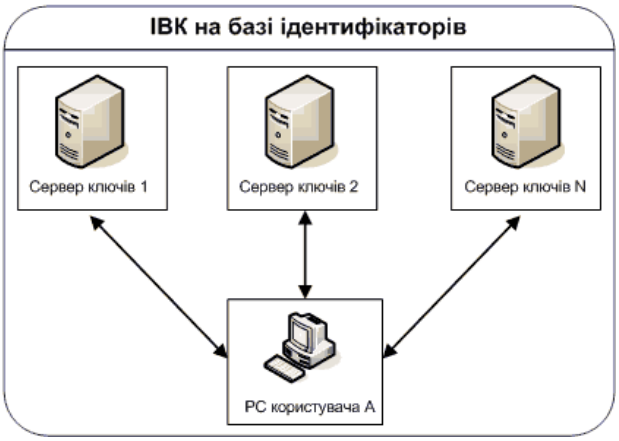

Рис. 6. Схема удосконаленого методу генерації ключів

Удосконалений метод генерації ключів визначається так:

Етап 1. Ініціалізація. Здійснюється у такій послідовності:

– налаштування та установка параметрів серверів генерації;

– налаштування забезпечення користувача та реєстрація користувача;

– виконання протоколу та вироблення за необхідністю ключів.

Налаштування та системна установка усіх УГК виконується так:

Усі n УГК разом обирають просте число q, дві групи G_1 , G_2 порядку q_i та білінійне відображення Вейля або Тейта $e : G_1 \times G_1 \to G_2$ та генератор групи $P \in G_1$. Далі обираються криптографічні геш-функції $H_1 : \{0,1\}^* \to G_1$ та $H_2 : G_2 \to \{0,1\}^l$ для деякого l.

Генерується майстер-ключ системи $S < p$, де $p-$ просте число, порядок групи точок ЕК. Будується многочлен $a_{n-1}x_i^{\left\lfloor \frac{n+1}{2} \right\rfloor - 1} + ... + a_1 x_i + S = 0$. Згідно з схемою Лагранжа, обчислюються частки s_i ключа для кожного сервера генерації. Кожен сервер генерації обчислює його відкритий ключ $P_i = s_i P$. Отже, будь-які $\left\lfloor \frac{n+1}{2} \right\rfloor$ з n УГК.

Обчислюється загальносистемний відкритий ключ $Y_N = SP$. Номери k_i кожного сервера запам'ятовуються.

Таким чином публікуються або є доступними для усіх користувачів такі загальносистемні параметри: $Params = \{G_1, G_2, e, H_1, H_2, P, P_0, P_1, ...P_n, k_1, k_2, k_n, Y_N\}$.

Етап 2. Реєстрація користувача. Користувач обирає відкритий ідентифікатор ID, обчислює відповідний відкритий ключ Q_{ID}, та виробляє довгостроковий секрет x. Далі користувач проходить реєстрацію на кожному сервері генерації та надає йому шляхом, що забезпечує цілісність, параметр xQ_{ID}, xP_i. Центр генерації перевіряє його правильність шляхом обчислення та перевірки умов: $e(xQ_{ID}, P_i) = e(Q_{ID}, xP_i)$, та зберігає дані, отримані від користувача у власній базі даних. Як результат, користувачу видається доказ реєстрації у вигляді $prf_{ID} = s_i H(ID \| xQ_{ID})$.

Користувач перевіряє отриманий доказ реєстрації, перевіряючи рівність $e(prf_{ID}, P) = e(H(ID \| xQ_{ID}), P_i)$.

Етап 3. Паралельний запит часткових ключів. Користувач здійснює запит до кожного ЦГ, надсилаючи йому кортеж $\{ID, x^{-1}P\}$.

Отримавши кортеж, ЦГ вибирає зі своєї БД xQ_{ID}, яке відповідає даному ID, та перевіряє справжність отриманої інформації, перевіряючи, що $e(x^{-1}P, xQ_{ID}) = e(P, Q_{ID})$. Якщо кортеж цілісний, то ЦГ множить значення xQ_{ID} на свій особистий ключ s_i та надсилає повідомлення $\{ID, s_i xQ_{ID}\}$ користувачу.

Етап 4. Вироблення та перевірка особистого ключа користувачем. Користувач, отримавши $t \geq k$ відповідей, обирає з них будь-які k, множить кожне на x^{-1} та отримує кортеж $(s_0 Q_{ID}, s_1 Q_{ID}, s_N Q_{ID})$.

Користувач будує систему рівнянь:

$$\begin{cases} a_{n-1}k_i^{n-1} + ... + a_1 k_i + a_0 = s_i Q_{ID} (\mathrm{mod}\, p) \\ a_{n-1}k_j^{n-1} + ... + a_1 k_j + a_0 = s_j Q_{ID} (\mathrm{mod}\, p), \\ a_{n-1}k_t^{n-1} + ... + a_1 k_t + a_0 = s_t Q_{ID} (\mathrm{mod}\, p) \end{cases} \quad (1)$$

Де s_i, s_j, s_t – особисті ключі серверів генерації, до яких звертався користувач, $a_0 = S$ – майстер-ключ системи (що був розподілений серверами генерації).

Користувач будує многочлен Лагранжа:

$$F(x) = \sum_i l_i(x) y_i (\mathrm{mod}\, p), \text{ де } \quad l_i(x) = \prod \frac{x - x_j}{x_i - x_i} (\mathrm{mod} p).$$

Користовач виконує підстановку значень k_i замість x_i, розв'язує систему (1), та отримує коєфіцієнти многочлена $a_{n-1}Q_{ID}, ... a_1 Q_{ID}, a_0 Q_{ID}$. Коефіцієнт $a_0 Q_{ID} = SQ_{ID}$ буде особистим ключем користувача.

Користувач перевіряє справжність отриманого особистого ключа SQ_{ID} шляхом перевірки такої рівності: $e(SQ_{ID}, P) = e(Q_{ID}, P_{sys})$. При позитивному результаті перевірки він приймає отриманий ключ як особистий.

Стійкість протоколу базується на інтерполяційній формулі Лагранжа, а також залежить від довжини модуля перетворень P і довжин S_i-х часток секрету. Розглянемо можливі атаки на схему Шаміра. Основною задачею атак є визначення загального секрету $S = a_0$. Значення a_0 можна визначити безпосередньо або через визначення значень приватних секретів $f(l_i), \ldots, f(l_k)$. Якщо $a_0 = S$ і формується довіреною стороною випадково, то складність атаки типу "груба сила" за визначенням a_0 можна оцінити через імовірність P_0 її здійснення

$$P_0 = \frac{1}{p-2} \approx \frac{1}{p} = p^{-1}. \quad (2)$$

Складність атаки "груба сила" за визначенням a_0 через значення $f(i_1), \ldots, f(i_k) \in GF(p)$ можна оцінити як

$$P_f = \left(\frac{1}{(p-1)^k} \right) = (p-1)^{-k} \approx p^{-k}. \quad (3)$$

Попередні порівняння (2) і (3) показують, що більш краща є атака за безпосереднім визначенням a_0. Складність цієї атаки залежить тільки від величини модуля p. Якщо p – відкритий загальносистемний параметр, відомий криптоаналітику, то складність атаки можна визначити також через безпечний час

$$T_б = \frac{I_0}{\zeta K} \approx \frac{p}{\zeta K}, \quad (4)$$

де $I_0 \approx p$ – число спроб підбору значення a_0 з імовірністю 1; ζ – продуктивність криптоаналітичної системи; $K = 3{,}1 \cdot 10^7$ с/рік – кількість секунд у році.

Доведено наступне твердження.

Твердження. Припустимо, що майстер ключ S розподілений на між n об'єктами, з яких $\left\lfloor \frac{n+1}{2} \right\rfloor$ мають змогу відтворити ключ, тобто використовується порогова схема Лагранжа $(\left\lfloor \frac{n+1}{2} \right\rfloor, n)$. Приймемо, що ймовірність успішної атаки на відмову в обслуговуванні на об'єкт дорівнює p, та усі атаки на об'єкти незалежні. Тоді ймовірність P не надання послуги доступність $\left\lfloor \frac{n+1}{2} \right\rfloor$ об'єктами оцінюється, відповідно для базового та удосконаленого методу, співвідношеннями $P = 1 - (1-p)^n$ та $P = \sum_{k=\left\lfloor \frac{n+1}{2} \right\rfloor}^{n} C_n^k \cdot p^k \cdot (1-p)^{n-k}$.

Показники доступності УГК для ймовірності $P = 0.1$ успішності атаки на відмову в обслуговуванні системи наведені у таблиці 1. За прототип узято метод Мелецького.

Таблиця 1

Показники доступності та компрометації

Прототип		Удосконалений метод	
Кількість серверів	Ймовірність виходу з ладу	Кількість серверів	Ймовірність виходу з ладу
2	0.19	2	0.19
3	0.27	3	0.028
4	0.34	4	0.0523
5	0.41	5	0.0085

На рис. 7 наведено графік залежності ймовірності виходу з ладу системи від ймовірності успішності атаки на відмову в обслуговуванні для п'яти серверів відповідно для базового (верхній) та удосконаленого (нижній) методів.

Результати розрахунків показали суттєве покращеня показників доступності, що вимірюється через ймовірність виходу з ладу системи за умови атаки на відмову в обслуговуванні на усі сервери генерації ключа.

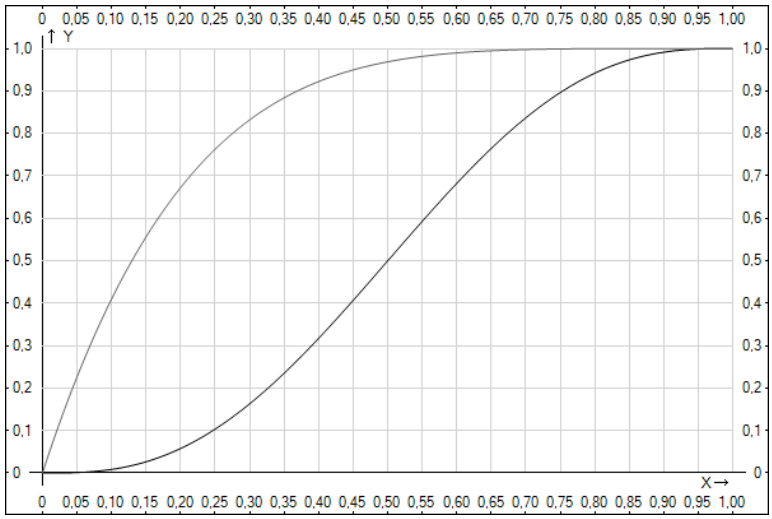

Рис. 7. Результати порівняння по критерію доступності

Зазначимо, що основними недоліками удосконаленого методу генерації ключів є збільшення компонентів системи для досягнення ймовірності компрометації, що властива прототипу. Проте рішення про застосування такої системи буде прийнято відповідно до вимог, що висуваються до неї.

У п'ятому розділі удосконалено метод аналізу безпеки криптопротоколів. Криптопротокол подається у формальному вигляді за допомогою наступних позначень:

Ключові дані $K ::= k \mid sh\,A \mid pk\,A \mid sk\,A$, ролі $r \in R$, повідомлення $M ::= . \mid R \mid N \mid K \mid F(M) \mid (M,M) \mid \{M\}_m$, базові типи $\tau ::= r \mid n\,(\text{nonce type}) \mid K$. Кожний блок інформації визначається як $tM ::= . \mid \tau \mid F(tM) \mid (tM,tM) \mid \{tM\}_{tM}$.

Формалізуються множини відправлених та отриманих даних tsend, trecv : $R \times R \times tM$, такі, що: $tsend(r,r',t_1) \wedge tsend(r,r',t_2) \Leftrightarrow tsend(r,r',(t_1,t_2))$ та $trecv(r,r',t_1) \wedge trecv(r,r',t_2) \Leftrightarrow trecv(r,r',(t_1,t_2))$, де $r,r' \in R, t,t_1,\ldots,t_n \in tM,\ f \in F$.

Для кожного учасника протоколу визначається специфікація ролі $TRoleSpec = \{t\,send_i(r,r',t), t\,recv_i(r,r',t) \mid t \in tM, i > 0, r,r' \in R\}$. Визначаються множини усіх відправлених та прийнятих для ролі даних $allsentMsgExluding_j(r') = \bigcup_{r' \in R, r'' \in R - \{r\}} \{t \mid send_i(r',r'',t) \in TProtSpec(r')\}$, де j – номер сеансу, та $recvdMsg_j(r) = \bigcup_{r' \in R} \{t \mid recv_i(r,r',t) \in TProtSpec(r)\}$ та усіх надісланих взагалі даних $allsentMsg_j = \bigcup_{r'.r'' \in R} \{t \mid send_i(r',r'',t) \in TProtSpec(r')\}$.

Удосконалений метод полягає у виконанні таких етапів:

1. Для кожної ролі $r \in R$ у сеансі протоколу визначити набори $allsentMsgExcluding_j(r)$, $recvdMsg_j(r)$, $allsentMsg_j$.

2. Визначити значення предиката REPLAY для $j = i$, такого що,

$REPLAY(r) \Leftrightarrow \exists\ t_r \in recvdMsg_j(r), t_s \in allsentMsgExcluding_i(r), t \in P(t_r), t' \in P(t_s)$,

тобто для одного сеансу протоколу.

3. Визначити значення предиката BASIC-TYPEFLAW такого, що

$$BASIC\_TYPEFLAW(r) \Leftrightarrow$$
$$\exists t_r \in recvdMsg_j(r), t_s \in allsentMsg_i, t \in P(t_r), t' \in P(t_s) \wedge$$
$$\exists t_1, t_2, t_3 \subset t, t_1', t_2' \subset t', f \in t, bt \in \tau - \{k\} \quad \text{при} \quad j = i.$$
$$t = \{t_1, k, t_2,\}_{f(t_3)} \wedge t' = \{t_1', bt, t_2',\}_{f(t_3)} \wedge |t_1| = |t_1'| \wedge |t_2| = |t_2'|$$

4. Визначити значення предиката REPLAY, такого що,

$$REPLAY(r) \Leftrightarrow \exists\ t_r \in recvdMsg_j(r), t_s \in allsentMsgExcluding_i(r), t \in P(t_r), t' \in P(t_s),$$

при $j \neq i$, тобто t' для різних сеансів протоколу (або протоколу з різними учасниками).

5. Визначити значення предиката BASIC-TYPEFLAW такого, що

$$BASIC\_TYPEFLAW(r) \Leftrightarrow$$
$$\exists t_r \in recvdMsg_j(r), t_s \in allsentMsg_i, t \in P(t_r), t' \in P(t_s) \wedge$$
$$\exists t_1, t_2, t_3 \subset t, t_1', t_2' \subset t', f \in t, bt \in \tau - \{k\} \quad \text{при} \quad j \neq i.$$
$$t = \{t_1, k, t_2,\}_{f(t_3)} \wedge t' = \{t_1', bt, t_2',\}_{f(t_3)} \wedge |t_1| = |t_1'| \wedge |t_2| = |t_2'|$$

За допомогою даного методу було проаналізовано протокол Ньюмана-Стабблемайн, та знайдено відому атаку. Таким чином, удосконалено метод аналізу безпеки криптопротоколів, який відрізняється від існуючого пошуком збігів термів у попередніх сеансах протоколу та сеансах протоколу з іншими учасниками, що дозволяє знайти протоколи, які не є криптоживучими.

ВИСНОВКИ

У дисертаційній роботі вирішено науково-технічну задачу розробки моделі та методів забезпечення послуг безпеки у комбінованих ІВК. Отримано такі наукові результати:

1. Нова модель комбінованої ІВК, у якої усі користувачі поділені на множини, що використовують цілісні унікальні загальносистемні параметри, політики безпеки та ідентифікатори користувачів, що дозволяє реалізувати модель взаємної недовіри і взаємного захисту.

2. Удосконалено метод направленого шифрування у комбінованій ІВК, для взаємодії користувачів з доменів, які не володіють погодженими загальносистемними параметрами, що відрізняється від існуючих отриманням і перевіркою загальносистемних параметрів та ідентифікатора отримувача, що дозволяє скоротити кількість необхідних операцій шифрування у 3 рази порівняно з прототипом.

3. Удосконалено метод генерації особистого ключа користувача для випадку розподіленого уповноваженого на генерацію ключів у ІВК на базі ідентифікаторів, який, на відміну від існуючих, передбачає паралельні запити користувача до серверів уповноваженого на генерацію ключів та формування особистого ключа безпосередньо користувачем, та дозволяє забезпечити доступність розподіленого уповноваженого на генерацію ключів у разі атаки типу “відмова в обслуговуванні”.

4. Удосконалено метод аналізу безпеки криптопротоколів, який відрізняється від прототипу порівнянням різних сеансів протоколу, що дозволяє виявити вразливості, властиві протоколам, які не є криптоживучими.

Результати дисертаційної роботи у ЗАТ “Інститут інформаційних технологій” (акт від 12.10.2011 р.) та у Харківському національному університету радіоелектроніки (акт від 14.10.2011 р.).

.

СПИСОК ОПУБЛІКОВАНИХ ПРАЦЬ ЗА ТЕМОЮ ДИСЕРТАЦІЇ

1.Горбенко І. Д. Проблемні питання та напрями розвитку інфраструктур з відкритими ключами / І. Д. Горбенко, Ю. І. Горбенко, О. Є. Ілясова, П. О. Кравченко, С. С. Батюшко, К. А. Погребняк //Сучасні та перспективні методи і моделі управління в економіці / ред. А.О. Єпіфанова. – Суми: ДВНЗ “УАБС НБУ”, 2008. – Ч.2. – С. 184–229.

2. Горбенко І. Д. Удосконалений протокол вироблення ключів з асиметричними криптографічними перетвореннями зі спарюванням точок еліптичних кривих на базі ідентифікаторів / І. Д. Горбенко, П. О. Кравченко, О. П. Мелецький // Научно-технический журнал "Радиотехника". – Х., 2006. – Вып. 147. – С.99–106.

3. Бондаренко М. Ф. Аналіз та перспективи сучасних протоколів видання та генерації ключів для інфраструктури на базі ідентифікаторів / М. Ф. Бондаренко, І. Д. Горбенко, О. П. Мелецький, П. О. Кравченко // Научно-технический журнал "Прикладная радиоэлектроника. Тематический выпуск, посвященный проблемам обеспечения информационной безопасности". – Х., 2007. – Том 6. – № 3. – С. 356–362.

4. Горбенко І. Д. Аналіз існуючих досліджень в галузі побудови комбінованої ІВК / І. Д. Горбенко, П. О. Кравченко // Научно-технический журнал "Прикладная радиоэлектроника. Тематический выпуск, посвященный проблемам обеспечения информационной безопасности". – Х., 2008. – Том 7. – № 3. – С. 267–270.

5. Бондаренко М. Ф. Комбінована інфраструктура відкритих ключів / М. Ф. Бондаренко, П. О. Кравченко // Научно-технический журнал "Прикладная радиоэлектроника. Тематический выпуск, посвященный проблемам обеспечения информационной безопасности". – Х., 2009. – Том 8. – № 3. – С. 327–329.

6. Горбенко І. Д. Комбінована інфраструктура відкритих ключів та її застосування / І. Д. Горбенко, П. О. Кравченко // Науково-технічний журнал "Радіоелектронні і комп’ютерні системи". – Х., 2009. – Вип. 5(39). – С. 86–90.

7. Горбенко І. Д. Безпека комбінованої схеми інфраструктури відкритих ключів для моделі випадкового оракула / І. Д. Горбенко, П. О. Кравченко // Науково-технічний журнал "Радіоелектронні і комп’ютерні системи". – Х., 2010. – Вип. 6(47). – С. 111–116.

8. Кравченко П. О. Результати порівняльного аналізу стандартів криптосистем на ідентифікаторах IEEE P1363.3, RFC 5091, RFC 5408 / П. О. Кравченко, Л. В. Макутоніна // Вісник Харківського національного університету. – Х., 2010. – № 926. – С. 139–146.

9. Кравченко П. О. Розширення моделі типізованої специфікації для формального аналізу криптографічних протоколів / П. О. Кравченко // Научно-технический журнал "Прикладная радиоэлектроника. Тематический выпуск, посвященный проблемам обеспечения информационной безопасности". – Х., 2011. – Том 10. – № 2. – С. 192–197.

10.Горбенко І. Д. Обгрунтування та вибір критеріїв та показників оцінки комбінованих ІВК / І. Д. Горбенко, П. О. Кравченко, Л. В. Макутоніна // Научно-технический журнал "Радиотехника". – Х., 2011. – Вып. 166. – С. 56–63.

11.Погребняк К. А. Модель комбінованої інфраструктури відкритих ключів / К. А. Погребняк, П. О. Кравченко // Автоматизированные системы управления и приборы автоматики: зб. наук. пр. – Х., 2011. – Вип. 155. – С. 53–61.

12.Кравченко П. О. Удосконалений метод генерації ключів для комбінованих інфраструктур відкритих ключів / П. О. Кравченко // Автоматизированные системы управления и приборы автоматики: зб. наук. пр. – Х., 2011. – Вип. 157. – С. 48–53.

13.Кравченко П. О. Розробка протоколів генерації та видачі ключів у криптосистемах на базі ідентифікаторів / П. О. Кравченко // Збірник наукових статей "Наукові доробки молоді – вирішенню проблем європейської інтеграції": тези докладів. – Х., 2007. – Том 1. – С. 241-242.

14.Кравченко П. О. Перспективная инфраструктура открытых ключей на идентификаторах и ее свойства / П. О. Кравченко, О. О. Козулін // XI Международная научно-практическая конференция "Безопасность информации в информационно-телекомуникационных системах": тези докладів. – К., 2008. – С. 90.

15.Кравченко П. О. Проблемні питання інфраструктур відкритих ключів на базі ідентифікаторів / П. О. Кравченко // 12-й международный молодежный форум "Радиоэлектроника и молодежь в XXI веке": Сб. материалов форума. – Х., 2008. – С. 17.

16.Бондаренко М. Ф. Комбінована інфраструктура відкритих ключів та її застосування / М. Ф. Бондаренко, П. О. Кравченко, О. О. Козулін // XII Международная научно-практическая конференция "Безопасность информации в информационно-телекомуникационных системах": тези докладів. – К., 2009. – С. 21–22.

17.Kravchenko P. Security analysis of IdComby identity-based encryption scheme / P. Kravchenko // Proceedings of the 10 International conference TCSET`2010, “Modern problems of radio engineering, telecommunications and computer science”, Lviv-Slavske, February 23-27, 2010

18.Горбенко І. Д. Аналіз стійкості комбінованої схеми інфраструктури відкритих ключів в моделі випадкового оракула / І. Д. Горбенко, П. О. Кравченко // XII Международная научно-практическая конференция "Безопасность информации в информационно-телекомуникационных системах": тези докладів. – К., 2010. – С. 31–32.

19.Kravchenko P. Development of improved key issuing protocol for the combined public key infrastructure / P. Kravchenko // Proceedings of the first International Workshop “Critical Infrastructure Safety and Security”. – Kharkiv, 2011. – V. 2. – P. 393-389.

АНОТАЦІЯ

Кравченко П. О. Модель та методи забезпечення послуг безпеки у комбінованих інфраструктурах відкритих ключів. – На правах рукопису.

Дисертація на здобуття наукового ступеня кандидата технічних наук за спеціальністю 05.13.05 – комп’ютерні системи та компоненти. – Харківський національний університет радіоелектроніки, Міністерство освіти і науки, молоді та спорту України, Харків, 2012.

Мета дисертаційного дослідження – розробка моделі та методів забезпечення послуг безпеки у комбінованій інфраструктурі відкритих ключів за рахунок використання унікальних загальносистемних параметрів та політик безпеки для множин користувачів. Основні результати: нова модель комбінованої ІВК, яка характеризується використанням унікальних загальносистемних параметрів та політик безпеки ІВК на базі ідентифікаторів для різних множин користувачів, забезпеченням цілісності ідентифікаторів і загальносистемних параметрів, що дозволяє реалізувати модель взаємної недовіри і взаємного захисту; удосконалено метод направленого шифрування у комбінованій ІВК, який відрізняється від існуючих протоколами отримання і перевірки загальносистемних параметрів та ідентифікатора отримувача, і дозволяє взаємодіяти користувачам, які не володіють погодженими загальносистемними параметрами, що дозволяє скоротити кількість необхідних операцій шифрування у 3 рази порівняно з прототипом; удосконалено метод генерації особистого ключа для комбінованої ІВК, який відрізняється паралельними запитами користувача до розподіленого уповноваженого на генерацію ключів та формуванням особистого ключа користувачем, що дозволяє збільшити показники доступності для розподіленого уповноваженого на генерацію ключів; удосконалено метод аналізу безпеки криптопротоколів, який відрізняється від існуючого пошуком збігів термів у попередніх сеансах протоколу та сеансах протоколу з іншими учасниками, що дозволяє знайти протоколи, які не є криптоживучими.

Ключові слова: криптографія, інфраструктура відкритих ключів, ідентифікатор, направлене шифрування, криптографічний протокол, безпечність криптографічних протоколів.

АННОТАЦИЯ

Кравченко П. А. Модель и методы обеспечения услуг безопасности в комбинированых инфраструктурах открытых ключей. – На правах рукописи.

Диссертация на соискание ученой степени кандидата технических наук по специальности 05.13.05 – компьютерные системы и компоненты. – Харьковский национальний университет радиоэлектроники, Министерство образования и науки, молодежи и спорта Украины, Харьков, 2012.

Цель диссертационного исследования – разработка модели и методов обеспечения услуг безопасности в комбинированной инфраструктуре открытых ключей за счет использования уникальных общесистемных параметров и политик безопасности для множеств пользователей. Сущность научного исследования заключается в разработке новой модели и методов обеспечения таких услуг безопасности как конфиденциальность, целостность и доступность в комбинированной инфраструктуре открытых ключей, что позволяет реализовать модель взаимного недоверия и взаимной защиты, существенно (в 3 раза) сократить количество необходимых операций шифрования для взаимодействия пользователей, которые не обладают согласованными общесистемными параметрами, обеспечить доступность распределенного уполномоченного на генерацию ключей в случае успешной атаки типа “отказ в обслуживании” на один из его компонентов. Решены задачи разработки модели комбинированной инфраструктуры открытых ключей, в которой все пользователи разделены на группы, обладающие целостными уникальными общесистемными параметрами, политиками безопасности, базами идентификаторов пользователей, позволяющей реализовать сквозное шифрование между пользователями различных групп; разработки усовершенствованного метода направленного шифрования, позволяющего использовать не согласованные общесистемные параметры для отправителя и получателя и соответствующего проктокола на его основе; разработки усовершенствованного метода генерации ключей для распределенной инфраструктуры открытых ключей на базе идентификаторов и соответствующего протокола на его основе; разработки усовершенствованного метода анализа безопасности криптографических протоколов.

Основные результаты: новая модель комбинированной инфраструктуры открытых ключей, которая характеризуется использованием уникальных общесистемных параметров и политик безопасности инфраструктуры открытых ключей на базе идентификаторов для различных множеств пользователей, обеспечением целостности идентификаторов и общесистемных параметров, что позволяет реализовать модель взаимного недоверия и взаимной защиты; усовершенствованный метод направленного шифрования в комбинированной инфраструктуры открытых ключей, который отличается от существующих протоколами получения и проверки общесистемных параметров и

идентификатора получателя, и позволяет взаимодействовать пользователям, которые не обладают согласованными общесистемными параметрами, что позволяет сократить количество необходимых операций шифрования в 3 раза по сравнению с прототипом; усовершенствованный метод генерации личного ключа для комбинированной инфраструктуре открытых ключей, который отличается параллельными запросами пользователя распределенному уполномоченному на генерацию ключей и формированием личного ключа пользователя, что позволяет увеличить показатели доступности для распределенного уполномоченного на генерацию ключей; усовершенствованный метод анализа безопасности криптопротоколов, который отличается от существующего поиском совпадений термов в предыдущих сеансах протокола и сеансах протокола с другими участниками, что позволяет найти протоколы, которые не являются криптоживучими.

Ключевые слова: криптография, инфраструктура открытых ключей, идентификатор, направленное шифрование, криптографический протокол, безопасность криптографических протоколов.

ABSTRACT

Kravchenko P.O. Model and methods of ensuring security in combined public key infrastructures. – Manuscript.

PhD thesis (candidate degree of technical sciences) in specialty 05.13.05 – Computer Systems and Components. – Kharkiv National University of Radio Electronics, Ministry of education and science, youth and sport of Ukraine, Kharkiv, 2012.

The aim of the research is to develop the model and methods of ensuring security in combined public key infrastructures by using the unique system parameters and security policies for sets of users. Main results: a new model of the combined public key infrastructure, which is characterized by using a unique system parameters and security policies for identity-based PKIs, ensuring the integrity of identifiers and system parameters, which allows to implement a model of mutual distrust and mutual protection; improved encryption method for the combined PKI, which differs mechanisms for check system parameters and receiver identifier, and allows users, which don’t have agreed system parameters, to interact and reduces the number of operations required for 3 times compared with the prototype; improved key-issuing method for the combined PKI, which differs from existing in parallel requests to the distributed private key generator and calculation of private key on user side and allows to increase rate of availability of distributed private key generator; improved method for security analysis of cryptoprotocols, which differs from the existing in matching terms in previous sessions of the protocol and protocol sessions with other participants, that allows to find protolols that are not forward secure.

Key words: cryptography, public key infrastructure, identifier, encryption, cryptoprotocol, security of cryptographic schemes.

Відповідальний випусковий В.М. Свищ

Підп. до друку 26.04.12. Формат 60x84 1/16. Спосіб друку – ризографія.

Умов. друк. арк. 1,2 Тираж 100 прим.
Ціна договірна. Зам. № 2-402.

ХНУРЕ. Україна. 61166, Харків, просп. Леніна, 14

Віддруковано в навчально-науковому
видавничо-поліграфічному центрі ХНУРЕ
61166, Харків, просп. Леніна, 14