матриц Фибоначчи // Научно-технический сборник «Коммунальное хозяйство городов". – К.: Техніка. – 2003. – Вып. 53. – С. 275 – 279.

УДК 681.3.06

ОСНОВНІ ПРИНЦИПИ ПОБУДОВИ ЦЕНТРІВ СЕРТИФІКАЦІЇ КЛЮЧІВ. ЦЕНТР СЕРТИФІКАЦІЇ КЛЮЧІВ „ДЖЕРЕЛО" ТА ЙОГО МОЖЛИВОСТІ

Іван Горбенко, Олена Качко, Олександр Волощук*, Дмитро Балагура, Сергій Головашич

*Харківський національний університет радіоелектроніки, *Укрсоцбанк*

Анотація: **Надаються основні терміни та поняття Законів України "Про електронний цифровий підпис" та "Про електронні документи та електронний документообіг" і задачі по створенню центрів сертифікації. Проводиться аналіз можливості використання центрів сертифікації Windows 2000 для цих центрів. Виконується аналіз архітектур центрів з урахуванням їх використання в розгалужених мережах. Описується центр сертифікації „ДЖЕРЕЛО".**

Summary: **Main term and concept of Law of Ukraine "About electronic digital signature" and "About electronic documents and electronic documents circulation" and tasks of creation of center certification are given. Analyze of possibilities of using certifications centers of Windows 2000 for this center is lead. Analyze of architectures of centers with taking into account their using in branchy networks is executes. Center certification "Jerelo" is described.**

Ключові слова: **Центр сертифікації, мережева модель, ієрархічна модель, електронний цифровий підпис, сертифікат.**

Вступ

В останній час багато документів почали розповсюджувати в електронному вигляді. В деяких державах, в тому числі і в Україні, у зв'язку с таким розвитком подій було прийнято закони, що дозволяють виконувати усі дії над документами у електронному вигляді, не вимагаючи їх переводу у тверді копії. В Україні такий Закон, повна назва якого "Про електронні документи та електронний документообіг"[1] було прийнято 22 травня 2003 року, а набув він чинності 22 листопада 2003 року. Головною метою закону є регулювання відносин, що виникають у процесі створення відправлення, передавання, одержання, зберігання, оброблення, використання та знищення електронних документів. Як виходить з вказаного вище Закону електронний документ – це документ, інформація в якому зафіксована у вигляді електронних даних, включаючи обов'язкові реквізити документа.

Для гарантування цілісності та справжності документа в електронному документі використовується цифровий підпис. Цифровий підпис, відповідно до Закону "Про електронні документи та електронний документообіг" [1], є "обов'язковим реквізитом електронного документа, який використовується для ідентифікації автора та/або підписувача електронного документа іншими суб'єктами електронного документообігу". Як можна зрозуміти з визначення терміну, цифровий підпис є невід'ємною частиною електронного документу, тому в той же день, що і Закон "Про електронні документи та електронний документообіг" було прийнято і Закон "Про електронний цифровий підпис"[2] – далі просто Закон. Закон дає таке визначення терміну електронний підпис. Електронний підпис – це дані в електронній формі, які додаються до інших електронних даних або логічно з ними пов'язані та призначені для ідентифікації підписувача цих даних. Електронний цифровий підпис – це вид електронного підпису, отриманого за результатом криптографічного перетворення набору електронних даних, який додається до цього набору або логічно з ним поєднується і дає змогу підтвердити його цілісність та ідентифікувати підписувача. Електронний цифровий підпис накладається за допомогою особистого ключа та перевіряється за допомогою відкритого ключа.

I Структура сертифікату

Закон "Про електронний цифровий підпис" встановлює вимоги до процесу виробки ключів, затвердження сертифікатів, їх розповсюдження та знищення. У відповідності до Закону сертифікат повинен містити такі обов'язкові дані:

- ✓ найменування та реквізити центру сертифікації ключів (центрального засвідчувального органу,

засвідчувального центру);

- ✓ зазначення, що сертифікат виданий в Україні;
- ✓ унікальний реєстраційний номер сертифіката ключа;
- ✓ основні дані (реквізити) підписувача власника особистого ключа;
- ✓ дату і час початку та закінчення строку чинності сертифіката;
- ✓ відкритий ключ;
- ✓ найменування криптографічного алгоритму, що використовується власником особистого ключа;
- ✓ інформацію про обмеження використання підпису.

Порівняння структури сертифікату відповідно Закону з структурою сертифікату відповідно X.509 показує, що перша структура відповідає другій.

II Задачі центрів сертифікації

Для виконання сертифікації ключів Законом передбачено декілька типів центрів сертифікації: центр сертифікації, акредитований центр сертифікації, засвідчувальний центр, центральний засвідчувальний орган. Основні розходження між вище означеними центрами – це рівень повноважень з видачі сертифікатів, а також по контролю за діями центрів нижчих рівнів. Розглянемо задачі, які повинні виконувати центри усіх рівнів. Центри сертифікації ключів мають надавати послуги електронного цифрового підпису та обслуговувати сертифікати ключів; отримувати та перевіряти інформацію, необхідну для реєстрації підписувача і формування сертифіката ключа безпосередньо у юридичної або фізичної особи чи у її уповноваженого представника; забезпечувати захист інформації в автоматизованих системах відповідно до законодавства; забезпечувати захист персональних даних, отриманих від підписувача, згідно з законодавством; встановлювати під час формування сертифіката ключа належність відкритого та відповідного особистого ключа підписувачу; своєчасно скасовувати, блокувати та поновлювати сертифікати ключів у випадках, передбачених Законом; своєчасно попереджувати підписувача та додавати в сертифікат відкритого ключа підписувача інформацію про обмеження використання електронного цифрового підпису, які встановлюються для забезпечення можливості відшкодування збитків сторін у разі заподіяння шкоди з боку центру сертифікації ключів; перевіряти законність звернень про скасування, блокування та поновлення сертифікатів ключів та зберігати документи, на підставі яких були скасовані, блоковані та поновлені сертифікати ключів; цілодобово приймати заяви про скасування, блокування та поновлення ключів; вести електронний перелік чинних, скасованих та блокованих сертифікатів ключів; забезпечувати цілодобово доступ користувачів до сертифікатів ключів та відповідних електронних переліків сертифікатів через загальнодоступні комунікаційні канали; забезпечувати зберігання сформованих сертифікатів ключів протягом строку, передбаченого законодавством для зберігання відповідних документів на папері. Центральний засвідчувальний орган, крім вищезгаданих функцій, повинен також виконувати функції формування та видачі посилених[2] сертифікатів ключів засвідчувальним центрам та центрам сертифікації і виконувати їх зберігання а також усі інші функції, які необхідно виконувати для звичайних сертифікатів.

III Структура центрів сертифікації

Виходячи зі вказаних вище задач, що повинні виконувати центри сертифікації ключів, їх структуру можна поділити на такі головні модулі (відповідно до PKI)[3]: сервер імен, орган реєстрації, центр генерації ключів, користувачі, орган сертифікації, архів, CRL, довідник сертифікатів.

Розглянемо більш детально функції кожного окремого модуля.

Сервер імен – контролює простір імен з метою видачі кожному абоненту унікального імені.

Орган реєстрації – несе відповідальність за авторизацію об’єктів. Його основна задача – перевірка змісту інформації в сертифікаті.

Центр генерації ключів – виконує генерацію пар відкритий/особистий ключ а також генерацію симетричних ключів та паролів. Центр генерації може бути як частиною програмного забезпечення органу сертифікації, так і частиною обладнання користувача чи довіреної третьої сторони.

Орган сертифікації – відповідає за організацію та виконання процесу сертифікації ключів (сертифікація, анулювання, нумерація сертифікатів та інше), а також гарантує їх справжність.

Архів – база даних, яка містить інформацію про сертифікати, строк дії яких вичерпано. Архів використовується для довгострокового зберігання сертифікатів які можуть знадобитися для перевірки

2 Посилений сертифікат – це сертифікат, який видано акредитованим центром сертифікації ключів, засвідчу вальним центром, центральним засвідчу вальним органом

документів, що були підписані на ключах, строк дії яких вже закінчився.

CRL – on-line перелік анульованих сертифікатів та сертифікатів, що блоковані, для сповіщення про зміни в сертифікатах абонентів.

Довідник (депозитарій) – база активних сертифікатів, доступ до якої організовано за системою on-line.

Але навіть якщо всі ці модулі будуть працювати окремо та на дуже потужних комп'ютерах, один єдиний центр з достатньою швидкістю навряд чи зможе обслуговувати навіть одну область, тому потрібна розгалужена система центрів, що взаємодіють між собою.

IV Моделі побудови мережі центрів

На сьогоднішній день існує три типи побудови мережі центрів: побудова по типу дерева (ієрархічна), побудова по типу мережі та комбінована схема, при якій кореневі центри дерев можуть бути об'єднані в мережу.

Кожна модель має свої переваги та недоліки.

Що стосується моделі з мережевою структурою, то основними перевагами такої структури є:

- ✓ Можливість прямої передачі сертифікатів між центрами будь-яких рівнів.
- ✓ Відпадає необхідність проводити пересертифікацію робочих ключів під час передачі між центрами.
- ✓ Сертифікат може бути перевірений будь-яким абонентом, незалежно від його підпорядкування, що на наш погляд є достатньо важливим аргументом на користь такої структури.

Серед недоліків структури такого типу можна відзначити:

- ✓ Необхідність виділення одного головного центру, який буде виконувати сертифікацію ключів усіх інших центрів сертифікації, у іншому випадку центри повинні проводити перехресну сертифікацію ключів.
- ✓ Необхідність усім центрам знати сертифікаційні ключі інших центрів, що приводить до значного зростання баз сертифікатів. У іншому випадку зростає завантаженість системи, що повинна передавати сертифікати між центрами не напряму, а через інші центри. Тоді середня довжина шляху, який повинен пройти ключ між двома буде складати $n = \frac{S}{2}$, де S - довжина шляху (у кількості передач між центрами), n - довжина максимального шляху між центрами (у кількості передач між центрами)
- ✓ Величезний обмін даними між центрами, які по запитам від інших центрів чи абонентів інших центрів повинні видавати сертифікати.

Якщо розглянути ієрархічну модель побудови центрів сертифікації, то для неї характерні наступні переваги:

- ✓ Повну підпорядкованість системи.
- ✓ Аналогічні мереженій моделі можливості по перевірці сертифікатів у разі відсутності системи поширення по адресам.
- ✓ Швидкодію системи по доступу до сертифікатів, якщо застосовується модель з пересертифікацією.
- ✓ Невеликий шлях сертифіката між двома центрами, який дорівнює сумі гілок по дереву між центрами, що зв'язуються.
- ✓ Невелика кількість ключів інших центрів сертифікації, якими повинен володіти центр.

Серед недоліків структури такого типу можна відзначити:

- ✓ Великий трафік з передачі ключів відразу після сертифікації, у тому випадку якщо відомо, що ключ буде використовуватися не лише локально. Цей недолік насправді може вилитись у перевагу у зв'язку з тим, що значно знижується кількість ключів, які необхідно передавати під час робочого використання ключів.
- ✓ Величезний об'єм бази при формуванні нового центру сертифікації у тому випадку, коли вже є достатньо розгалужена та об'ємна система центрів сертифікації та велика кількість ключів.
- ✓ Необхідність пересертифікації ключів у випадку, якщо система використовує модель, у якій абонент центру сертифікації знає тільки свій ключ сертифікації.

Комбінована схема має переваги мережевої та ієрархічної систем, але збільшується навантаження на кореневі центри, які самі по собі повинні бути розподіленими системами.

Тому можна сказати, що найбільш вірною для невеликих відкритих систем сертифікації є мережева модель. Якщо система сертифікації є внутрішньою, корпоративною або банківською, то можна однозначно вважати найбільш придатною до застосування систему ієрархічного типу з системою поширення сертифікатів по адресам. Якщо створюється система PKI для групи самостійних підрозділів, тим більше для загальнодержавного масштабу, то використовується комбінована схема.

Аналіз типів та функціонального навантаження центрів, які введені Законом дозволив нам зробити висновки щодо способу побудови мережі центрів сертифікації в загальнодержавному масштабі. Як вже зазначалося вище, Закон вимагає створення центрів чотирьох типів: центральний засвідчувальний орган,

засвідчувальні органи, акредитовані центри сертифікації, центри сертифікації. Закон визначає, що всі центри, що не підпорядковуються засвідчувальним центрам (тобто не є внутрівідомчими) виконують сертифікацію свого ключа у центральному засвідчувальному органі. Всі центри, що підпорядковуються засвідчувальному органу виконують сертифікацію свого ключа у цьому засвідчувальному органі. Такий варіант засвідчення чинності ключів сертифікації центрів повністю відповідає ієрархічній структурі побудови центрів, тобто відносно сертифікаційних ключів усі центри будуть побудовані по ієрархічній структурі, в якій центром першого рівня (головним центром) буде центральний засвідчувальний орган. Центрами другого рівня будуть засвідчувальні органи, акредитовані центри, центри сертифікації, вони підпорядковуються центральному засвідчувальному органу. Крім того, засвідчувальним органам можуть бути підпорядковані внутрішні центри сертифікації. Під підпорядкованістю у даному випадку розуміється засвідчення центром верхнього рівня чинності ключа підпорядкованого центра. Якщо в системі буде кілька засвідчувальних органів, система буде відповідати комбінованій архітектурі.

Всі центри (акредитовані та центри сертифікації) відносно робочих ключів будуть організовані у мережеву структуру, що дозволить напряму виконувати обмін сертифікатами робочих ключів. Ми вважаємо, що кожен центр може зберігати у себе деяку, визначену раніше, кількість чужих ключів та необмежену кількість ключів, що сертифіковані безпосередньо цим центром сертифікації. Сховище чужих ключів будемо називати кеш сертифікатів. Вибір чужих ключів для зберігання в кеші може виконуватися за наступними критеріями (стандартними для роботи з кешом комп'ютера): ключ, що сертифікований іншим центром сертифікації, може потрапити до кеша тільки у тому випадку, коли він потрібен абоненту даного центра для роботи. Якщо кеш повністю заповнений, а до нього необхідно занести ключі, виконуються дії, які дозволяють визначити як давно не приходили запити на той чи інший ключ і як часто тим чи іншим ключем користуються абоненти. На основі цього аналізу ключі, що давно не використовувались та/або запити на які приходять рідко видаляються з кеша та на їх місце заносять необхідні ключі. Крім того, можна виконувати періодичний аналіз кеша і видалення непотрібних ключів у моменти відсутності навантажень на центри сертифікації.

V Огляд існуючих центрів сертифікації

Для прийняття рішення про необхідність та особливості побудови центрів сертифікації у складі, визначеному Законом, нами було оглянуті існуючі центри сертифікації ключів, для яких визначена архітектура, а саме UniCERT is Baltimore Technologies' flagship product, центри сертифікації Windows 2000, ... Як показав огляд архітектури цих центрів, вони складаються з блоків, функції яких відрізняються не суттєво, відрізняється в основному тільки термінологія. Тому в подальшому ми будемо розглядати тільки центри сертифікації Windows 2000 з урахуванням доповнень для Windows 2003. При необхідності отримання сертифікату клієнт звертається в службу реєстрації, яка виконує аутентифікацію клієнта та перевірку його прав. Якщо запит клієнта визнано як припустимий, він передається в службу сертифікації, яка створює ключову пару, сертифікат відповідно запиту, та записує отримані дані в службу каталогів Active Directory. Адміністратор домену задає політику безпеки для системи. Windows 2000 дозволяє створити центр сертифікації підприємства, який може обслуговувати кілька систем у тому сенсі, що користувач може використовувати один ключ для роботи з різними системами. Усі центри Windows 2000 розподіляє на кореневі, ті, що видають та проміжні. Центри першого типу – це центри самого верхнього рівня дерева, довіра до усіх других центрів цього дерева базується на довірі цьому центру. Центри другого типу видають сертифікати клієнтам, центри третього типу видають сертифікати іншим центрам і не являються кореневими центрами. Декілька дерев можна об'єднати в одну систему, яка називається лісом (forest).

З цього короткого огляду видно, що структура центрів відповідає ієрархічній моделі, можна використовувати комбіновану модель. Windows 2000 вміщує набір компонентів, які дозволяють побудувати центр сертифікації потрібної структури. Створені ключі та сертифікати можна використовувати в системних компонентах Windows 2000, таких як Microsoft Office, Microsoft Outlook, та ін. Програмне забезпечення Windows 2000 дозволяє використовувати ключі та сертифікати в програмних продуктах користувача.

Це позитивні риси центру сертифікації Windows 2000.

Розглянемо характеристику цих центрів по наступним критеріям.

- ✓ Можливість використовувати національну криптографію в центрах сертифікації ключів.
- ✓ Забезпечення достатньої стійкості системи.
- ✓ Можливість гнучкого керування розподілом ключових даних в системі з урахуванням стану мереж на Україні.
- ✓ Зберігання особистого ключа.

По першому критерію. Центр сертифікації Windows 2000 використовує криптопровайдери для виконання усіх криптографічних функцій. Система дає змогу вибрати криптопровайдер для використання. WinApi включає функції для створення криптопровайдеру користувачем. Але криптопровайдер, що створений, необхідно підписати в фірмі Microsoft для того, щоб система її прийняла, як свою утиліту. На Україні немає правових норм, які визначають цю процедуру. Тому сьогодні не можливо зареєструвати криптопровайдер для його використання Центром сертифікації Windows 2000.

По другому критерію. Модулі центру сертифікації Windows 2000 і криптопровайдер реалізовані як окремі DLL. Так, наприклад, модуль керування заявками реалізовано в Xenroll.dll. З боку гнучкості системи для розробників це найкраще рішення. Але це рішення не забезпечує стійкості системи. Є багато робіт, які показують, яким чином можна змінити функціональність динамічних бібліотек, у тому числі, криптопровайдера, наприклад [4, 5]. Тому при розробці центрів сертифікації ключів, довіра до яких повинна бути дуже високою, використання DLL для базових модулів системи вважаємо недоцільним. Крім того, система використовує свої стандартні модулі для роботи з центром, наприклад, результати роботи модулю реєстрації користувача в системі (вхід в систему) використовується для реєстрації користувача в криптосистемі. Відомо багато нарікань на ці модулі.

По третьому критерію. Microsoft використовує дуже зручний механізм Active Directory, який забезпечує сумісний захищений доступ до сертифікатів усіх користувачів системи. Цей апарат дозволяє не використовувати або суттєво спростити дуже складну процедуру доставки сертифікатів. Але він потребує надійних мережених та міжмережених сполучень. Це не відповідає стану мереж на Україні сьогодні. Крім того, це робить систему значно дорожчою у використанні, тому що потребує постійної підтримки online з'єднання. Механізм експортування ключів частково вирішує цю проблему, але в цьому разі доставкою сертифікатів повинен займатись кінцевий користувач, що робить систему незручною для нього, або сертифікат відсилається разом з захищеним повідомленням, що в багато разів перевантажує канал передачі даних. Тому вважаємо, що разом з використанням Active Directory потрібно мати інші методи розповсюдження ключів. Найбільш зручним та дешевим для користувача методом вважаємо метод захищеної доставки ключа за заявкою користувача, забезпечення його актуалізації та захищеного зберігання в його локальному сховищі. У разі використання локальних сховищ можливо розглянути 2 варіанти. Перший варіант передбачає зберігання відкритих ключів сертифікації усіх проміжних центрів, з користувачами яких виконується робота. Другий варіант передбачає перепідпис ключів при їх проходженні через відповідні центри. Перший варіант передбачено центром сертифікації Microsoft. В цьому випадку в локальній базі даних будуть зберігатися відкриті ключі користувачів, які підписані різними центрами. В спеціальній базі будуть зберігатися відкриті ключі відповідних центрів. Можна використовувати наступний алгоритм опрацювання повідомлень[3].

Шаг 1. Визначення користувача, який надіслав повідомлення, і його центра.

Шаг 2. Пошук та зчитування відкритого ключа його центра.

Шаг 3. Перевірка сертифіката.

Шаг 4. Перевірка цифрового підпису повідомлення.

Шаги 1-4 треба повторювати для кожного повідомлення.

В другому варіанті в локальній базі зберігаються ключі користувачів, які підписані одним і тим же ключем. Необхідність в зберіганні ключів сертифікації інших центрів відпадає. Крім того, відкритий ключ свого центру може бути прочитано один раз при ініціюванні системи. Алгоритм опрацювання повідомлення у другому варіанті наступний:

Шаг 1. Визначення користувача, який надіслав повідомлення.

Шаг 2. Перевірка його сертифіката.

Шаг 3. Перевірка цифрового підпису повідомлення.

Таким чином, у другому варіанті зменшуються локальні бази та час, який потрібен на обробку кожного повідомлення.

По четвертому критерію. Не дивлячись на довіру центру сертифікації, кожний господар особистого ключа може бути впевнений в його недоторканності, якщо цей ключ формується особисто ним, зберігається на надійному носії і не передається ні в якому разі по системі. Відповідно встановленій політиці Центр сертифікації Windows 2000 може забезпечити режим, коли користувач сам формує свої ключі. Але центр включає модуль відновлення центру та ключових даних. Цей модуль не може працювати без передачі особистих ключів. Крім того, для забезпечення можливості відновлення в системі використовується стандартний модуль резервного копіювання, таким чином, особистий ключ не тільки передається до центру, а і зберігається в резервних копіях. У зв'язку з тим, що модуль резервного

3 Передбачається, що усі потрібні сертифікати вже знаходяться в локальних базах

копіювання не створювався для захищеного зберігання ключових даних, надійність цього зберігання викликає сумнів.

Таким чином, використання центру сертифікації Windows не відповідає сучасним потребам в побудові центрів сертифікації.

VI Особливості побудови центрів сертифікації

Розглянемо внутрішню структуру кожного із типів центрів, які визначаються Законом. Структура центрів, на наш погляд, буде відрізнятися головним чином ступінню безпеки та типом ключів (робочі, сертифікаційні), з якими вони будуть працювати. Узагальнену схему структури центру сертифікації було затверджено у стандарті ISO/IEC 11170 [3], вона має такий вигляд (див. рис. 1).

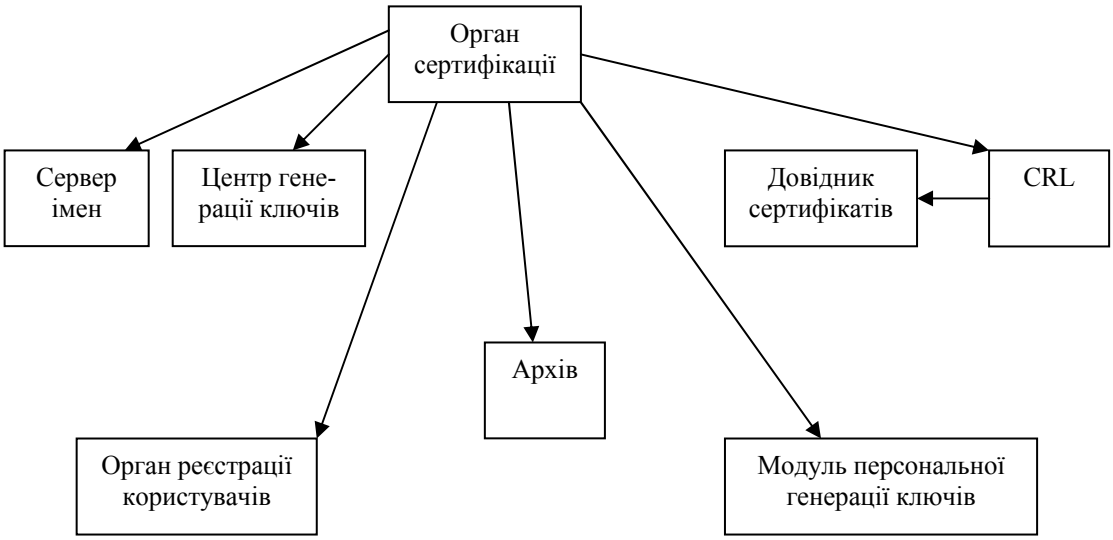

Рисунок 1 - Узагальнена схема структури центру сертифікації

Проведемо аналіз можливостей та властивостей, якими мають володіти центри сертифікації ключів як корпоративних та банківських систем, так і відкритих систем.

У будь-якій системі формування, обробки та використання ключів найважливішим моментом роботи системи є безпека ключових даних. Для відкритих ключів це цілісність та справжність, для особистих ключів це, насамперед, конфіденційність. Тому центри сертифікації, на наш погляд повинні надавати наступні можливості стосовно особистих ключів:

1) використання для збереження секретної ключової інформації різні носії. Це означає, що крім дискет існує необхідність у використанні альтернативних носіїв, наприклад, Touch-карти, USB модулі пам'яті.

2) необхідність надання можливості користувачам персонально генерувати собі ключі та за допомогою інструментів центру виконувати дії по їх відправці на сертифікацію та отримання сертифікатів та підтверджень.

3) можливість для користувача використання одного ключа у декількох системах з різними можливостями.

Розробка і аналіз структури центру сертифікації ключів дозволили нам рекомендувати такий спосіб реалізації вимоги пункту 3, вказаного вище. Кожен користувач системи під час формування профілю свого ключа (або, найчастіше, адміністратор системи під час формування профілю ключа користувача) вказує для ключа кількість та найменування систем, в яких у користувача буде можливість використовувати свій робочій ключ, а також перелік ролів, які буде виконувати цей ключ.

Також важливою задачею для центра сертифікації є підтримання безперервності дії ключів користувачів. Тут під безперервністю ми розуміємо не можливість постійного доступу до відкритого

сертифіката робочого ключа, а можливість зміни ключів без зупинки роботи користувача. Таку можливість може забезпечити центр сертифікації, що підтримує формування та сертифікації нових ключів ще до закінчення часу використання діючих ключів. Тобто центр має підтримувати можливість зберігання декількох ключів одного користувача, з яких тільки один ключ є дійсним у даний момент часу.

Тепер розглянемо систему безпеки центру. Вона є не менш важливою складовою частиною працездатності центру. Система безпеки повинна охоплювати всі модулі та контролювати всі дії, які виконує центр сертифікації ключів. Вона може складатися з наступних частин: система контролю доступу до основних модулів програми, система контролю та керування доступом до виконання головних (критичних) функцій програми, система підтримання і контролю вірності конфігурації програми та окремих її модулів, система протоколювання дій обслуговуючого персоналу. Крім того задля забезпечення більшої безпеки системи та виключення можливостей зловживання персоналу центру можна програмно, територіально та адміністративно поділити функції центру як це передбачено інфраструктурою відкритих ключів PKI. Система контролю доступу до основних модулів програми, система контролю та керування доступом до виконання головних (критичних) функцій програми може бути виконана за допомогою парольних функцій або функцій доступу за наявності ключового носія. Тут під критичними функціями ми розуміємо функції, що призводять до зміни конфігурації системи або конфігурації користувачів, функції, що виконують генерацію та сертифікацію ключів. Система підтримання і контролю вірності конфігурації програми та окремих її модулів може бути виконана на основі системи бінарного контролю за цілісністю файлів, що входять до складу системи. Система протоколювання дій обслуговуючого персоналу може бути виконана як система ведення журналів, у які заносяться всі дії системи та персоналу.

Підводячи підсумки аналізу структури центрів сертифікації ключів, можна сказати, що у будь-якому випадку структура побудови мережі центрів сертифікації повинна розроблятись в залежності від системи, яку вона має обслуговувати. Так, для систем, що мають обслуговувати банківські мережі необхідно використовувати центри сертифікації, які побудовані в ієрархічну структуру. У разі використання центрів сертифікації для роботи с ключами, що використовуються для захисту електронної пошти необхідно використовувати мережену структуру центрів. У деяких окремих випадках структура побудови центрів може бути комбінованою.

З урахуванням вимог до системи центрів, які визначає Закон, і критеріїв, визначених в пункті 5 цієї роботи, розроблена система ЦУСК „Джерело” . В системі „Джерело” використовується національна криптографія. За допомогою DLL реалізовані лише допоміжні функції, такі як керування зовнішніми пристроями для ключів (керування touch memory, Etoken, RuToken). Ключі на цих носіях зберігаються в зашифрованому вигляді, їх розшифровка виконується особистими модулями програми, а не DLL, тому використання DLL для цих цілей виправдано. В якості сховища для сертифікатів використовується локальна база даних, система керування якою є компонентом системи „Джерело”. В цьому компоненті використані допоміжні заходи захисту ключових даних відповідно [6]. Ключову пару формує тільки господар ключа, для чого використовує спеціальний компонент. Особистий ключ завжди записується на індивідуальний ключовий носій (використовувати для нього жорсткий диск система не дозволяє). Внутрішніми засобам системи можна створити декілька копій особистого ключа на різних ключових носіях. Це забезпечує можливість відтворення інформації, якщо оригінал особистого ключа не може бути використаним.

VII Узагальнена структура ЦУСК „Джерело”

Розглянемо які модулі існують в ЦУСК „Джерело”. Центр має три головних модуля – це, власне, центр управління і сертифікації ключів, модуль (програма) управління конфігурацією центрів та генераторів клієнтів, генератори клієнтів. Якщо порівняти функції модулів системи “Джерело” та компонентів центра сертифікації PKI, то орган реєстрації користувачів – це програма адміністратора безпеки; сервер імен, центр генерації ключів, орган сертифікації, довідник сертифікатів, архів, CRL, центр сертифікації – це центр вищого рівня та центри нижчих рівнів; крім того, модулі персональної генерації ключів – генератори ключів системи “Джерело”. Схема відповідності між модулями структури PKI та модулями центра “Джерело” та взаємодії між ними надана на рис. 2. Для використання робочих ключів використовуються робочі місця та спеціалізовані модулі, що функціонують під різними операційними системами.

Як вже вказувалось вище, система “Джерело” є ієрархічною системою, тому вона жорстко контролює свою структуру (див. рис.3). Саме через цю властивість у центр була додана програма формування дерева центрів. Ця програма додана для розподілення повноважень та відповідальності. Оператором програми є адміністратор безпеки головного центру. Тільки в програмі формування дерева існує можливість додавати до структури дерева центри будь-якого (але, зрозуміло, не першого) рівня. Крім того, програма

формування дерева головного центра дозволяє додавати робочі місця у головному центрі, генератори, що будуть підпорядковані безпосередньо цьому центру та робочі місця для них. Аналогічні модулі зміни конфігурації дерева є у кожного з центрів нижчих рівнів, але їх можливості обмежуються тільки додаванням робочих місць персонально для цього центру та генераторів, підпорядкованих цьому центру та робочих місць для них, тому для роботи з модулями формування дерева в центрах нижчих рівнів не потрібні окремі співробітники і, взагалі, ці модулі є невід'ємною частиною центрів. Для будь-якого центру можна сформувати довільну кількість робочих місць та довільну кількість генераторів. Те саме й для генераторів: для них також можна сформувати довільну кількість робочих місць. На рис. 3 зображені лише два рівня центрів сертифікації, насправді ж центрам другого рівня можуть підпорядковуватися центри третього рівня, центрам третього рівня можуть, відповідно підпорядковуватися центри четвертого рівня і так далі. Кількість рівнів у системі необмежена, але, насправді, перебільшення достатньої кількості рівнів тільки невиправдано ускладнять роботу системи. В результаті аналізу та експлуатації системи ми прийшли до висновку, що для абсолютної більшості корпоративних та банківських мереж достатньо три, максимум чотири рівні.

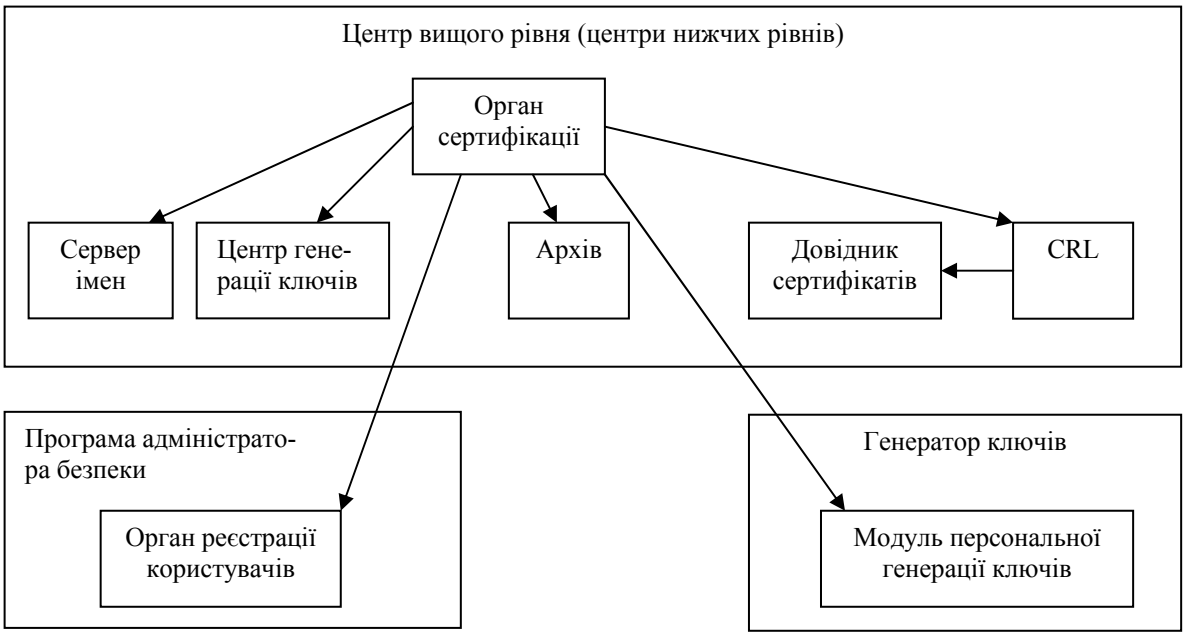

Рисунок 2 - Схема відповідності між модулями структури PKI та модулями центра "Джерело"

Розгортання системи по рівням виконується наступним чином. Після встановлення головного центру, адміністратор безпеки формує дерево центрів і передає його головному центру. В головному центрі після прийому структури дерева центрів виношується формування інсталяційних пакетів для центрів другого рівня. Центри другого рівня після встановлення формують інсталяційні пакети для центрів третього рівня і так далі. Такий порядок встановлення центрів було закладено тому, що центри другого рівня та нижче можуть „спілкуватись" (вести передачу ключів та іншої службової інформації) тільки з центрами, яким вони безпосередньо підпорядковуються, або які безпосередньо підпорядковуються їм. Кожен центр, формує інсталяційні пакети для своїх підлеглих генераторів.

Після встановлення центру будь-якого рівня і реєстрації ключа сертифікації (для всіх центрів, крім головного) центр може формувати для себе і своїх генераторів (клієнтів) робочі місця. Робоче місце в центрі чи генераторі являє з себе запис, у якому зазначаються назва робочого місця, прізвище володаря ключа, дії, які можна виконувати з цим ключем (підпис чи підпис та шифрування), список розсилки ключа, та ролі, які може виконувати володар ключа. На останніх двох пунктах ми зупинимося більш детально нижче.

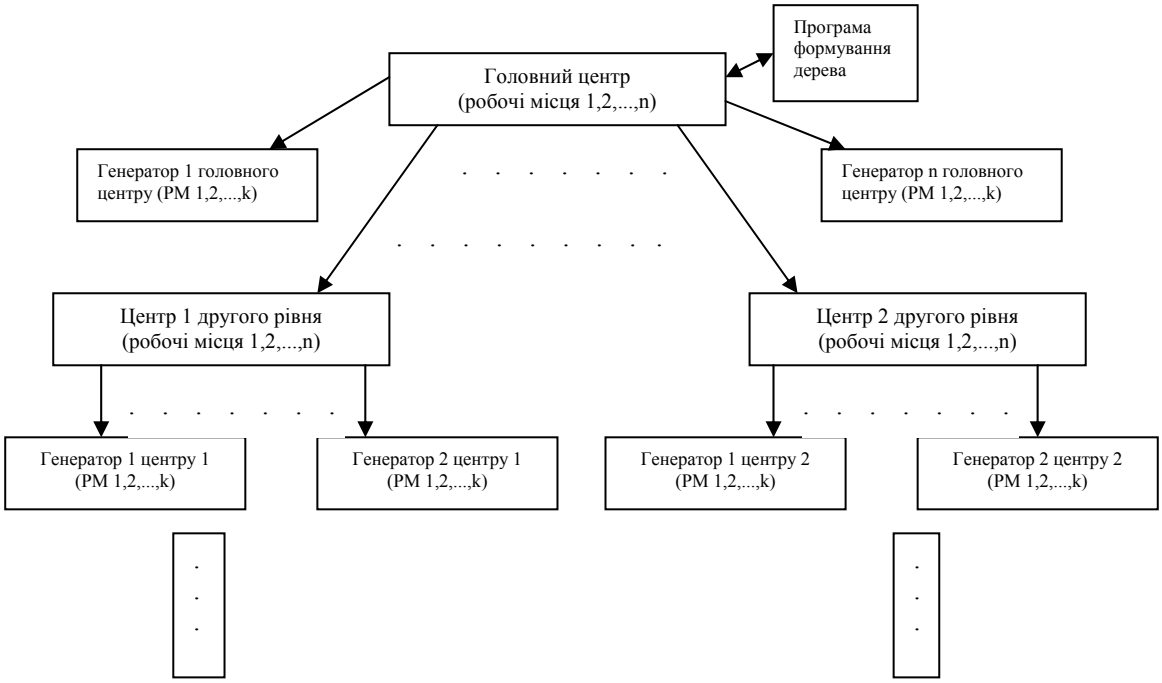

Рисунок 3 – Структура ієрархічної системи центру „Джерело”

VIII Ключова структура ЦУСК „Джерело”

Розглянемо ключову структуру системи “Джерело”. Головним ключем системи є сертифікаційний ключ центра вищого рівня. За допомогою цього ключа центр підписує усі робочі ключі абонентів, підпорядкованих безпосередньо цьому центру а також сертифікаційні ключі центрів, підпорядкованих йому. Для зв’язку між центрами, що підпорядковані між собою безпосередньо, та між генераторами і центрами центри верхніх рівнів разом з інсталяційними пакетами формують транспортні ключі. На цих ключах і на ключах сертифікації відбувається шифрування та підпис усіх ключових та службових даних, що проходять між центрами безпосередньої підпорядкованості. Якщо необхідно передати дані між центрами, що знаходяться на різних гілках дерева центрів, то передача ключових даних проходить через центр найнижчого рівня, який є загальним для обох центрів, що спілкуються. При цьому, кожен центр, через який проходить передача, перешифровує файли для подальшої передачі. Передача даних може виконуватися двома способами – передача через файли (у цьому випадку вхідні та вихідні файли формуються у заданих директоріях) та передача електронною поштою (у цьому випадку центр сам відправляє файли електронною поштою на електронну адресу абонента і автоматично приймає призначені йому файли).

Робочі ключі. Робочі ключі в системі можуть формуватися безпосередньо в центрах сертифікації ключів. Але для клієнтів банківських систем найбільш прийнятним є формування ключів персонально клієнтами (власниками ключів) за допомогою генераторів ключів. Кожен ключ має свій список розсилки – інформацію, у якій вказується, кому має бути передано сертифікат відкритого ключа (хто з абонентів у подальшому зможе обмінюватись інформацією те перевіряти підпис володаря цього ключа). Система не підтримує перевірку сертифікатів за допомогою сертифікаційних ключів інших центрів, тому коли центр отримує ключ, що сертифікований іншим центром, він виконує його пересертифікацію. Це означає, що після того, як центр отримав ключ та перевірив правильність сертифіката він виконує сертифікацію отриманого ключа за допомогою свого ключа сертифікації. Серед важливих особливостей системи можна вказати можливість використовувати різні носії для секретних ключів: звичайні дискети, COM та USB носії. Система дозволяє записувати на різні типи носіїв як робочі, так і сертифікаційні ключі, що актуально, якщо звернути увагу на надійність дискет. Як вже відзначалося вище, система підтримує формування списку ролей для кожного ключа. Це означає, що кожен ключ, що формується в системі у разі необхідності може бути використаний у декількох системах безпеки. Наприклад, якщо центр обслуговує систему клієнт-банк та систему захищеної пошти, то користувачу для роботи в обох системах не потрібно

буде генерувати окремі ключі. В такому випадку адміністратору безпеки центру необхідно буде під час формування запису про робоче місце вказати, що ключ цього робочого місця може використовуватися відразу у декількох системах та вказати ролі, які буде виконувати цей ключ. Необхідно відзначити, що набір систем та ролей не є фіксованим, а може бути модифікований у центрі верхнього рівня. При інсталяції центрів нижчого рівня та генераторів система проконтролює правильність формування списків ролей та систем та виконає синхронізацію.

Сертифікати. Сертифікати центр зберігає у захищеній базі даних власного формату, що не може бути прочитана стандартними системами керування базами даних. Сертифікати по інформації, що входить до їх складу, відповідають стандарту X.509. База сертифікатів підписується та хешується, крім того, кожен відкритий сертифікат шифрується та хешується. У базі сертифікатів можуть зберігатися як дійсні сертифікати, так і нові, що ще тільки мають вступити у дію, та щойно видалені. Центр має змогу заблокувати роботу сертифікату, якщо виникла підозра на компрометацію відповідного секретного ключа.

IX Система безпеки ЦУСК „Джерело”

Розглянемо тепер систему безпеки центру сертифікації. Для доступу до системи необхідно мати пароль. Крім того, навіть після входу у систему, основні дії можна виконати, тільки за допомогою носія з ключем сертифікації. Функції зміни структури системи контролюються адміністратором безпеки, який також має персональний ключ для роботи зі структурою системи. Сертифікат включає в себе поля лічильників цифрового підпису та шифрування, що захищає систему від можливості оновлення системи після виконання деяких операцій. Усі дії, починаючи від запуску системи і до завершення роботи програми заносяться у журнал операцій центра, де записуються такі дані: час, фамілія відповідального, найменування операції, над чим проводилась (якщо треба), статус виконання операції. Журнали та центр разом з іншими службовими файлами контролюються на цілісність.

Висновки

Надаються основні терміни та поняття Законів України “Про електронний цифровий підпис” та “Про електронні документи та електронний документообіг” і задачі по створенню центрів сертифікації. Проводиться аналіз можливості використання центрів сертифікації Windows 2000 для цих центрів. Виконується аналіз архітектур центрів з урахуванням їх використання в розгалужених мережах. Описується центр сертифікації „ДЖЕРЕЛО”

Відповідно законам [1], [2] в Україні повинні бути створені Центральний засвідчу вальний орган, Центральний та відомчі Засвідчувальні центри, Акредитовані центри, та центри сертифікації ключів. Виконано аналіз можливості використання центрів сертифікації ключів Windows 2000 для цих центрів. Аналіз показав, що використання цих центрів неможливо. Визначена архітектура системи, яка відноситься до комбінованих систем. Ця система складається з декількох ієрархічних систем. Наведена структура, функції, можливості використання система „ДЖЕРЕЛО” в якості центрів сертифікації всіх рівнів відповідно [2] для банківських та корпоративних мереж.

УДК 638.235.231

О ПРИМЕНЕНИИ КРИПТОГРАФИЧЕСКИХ СРЕДСТВ ОС WINDOWS ДЛЯ МАСКИРОВАНИЯ ИНФОРМАЦИИ

Евгений Клименко
НИЦ “ТЕЗИС” НТУУ “КПИ”

Анотация: **Рассматриваются вопросы применения криптографических средств, совместимых с ОС Windows, для защиты информации, циркулирующей в компьютерных системах.**
Summary: **Considered questions of the using the cryptographic facilities compatible with OS Windows.**
Ключевые слова: **Криптография, криптографические интерфейсы, ключи, энтропия, Crypto API, PGP SDK.**

Введение

Задачи защиты информации, циркулирующей в компьютерных системах всегда актуальны. Прежде всего, это связано с возросшей популярностью т.н. «сильно распределенных» приложений, состоящих из