Розділ 9

СИСТЕМА ЕЦП УКРАЇНИ ТА ЇЇ ЗАСТОСУВАННЯ

9.1. НОРМАТИВНО-ПРАВОВА БАЗА СТВОРЕННЯ ТА ЗАСТОСУВАННЯ СИСТЕМИ ЕЦП В УКРАЇНІ

У 2003 році в Україні було прийнято, а з 1 січня 2004 року надано чинності Законам України «Про електронний цифровий підпис» та «Про електронні документи та електронний документообіг» [2–3]. Ці документи заклали основу створення систем електронного цифрового підпису як у державному масштабі, так і на корпоративному рівні, на рівні окремих інформаційно-телекомунікаційних систем тощо. Для ефективного використання та якісного надання послуг ЕЦП необхідно вирішувати багато технологічних і технічних проблем.

Аналіз практичного досвіду впровадження технологій електронного документообігу [57–60, 113], технологій інфраструктури відкритого ключа зарубіжних країн [5, 51, 63–73, 81–83, 146–157, 220–234], практичний досвід вітчизняних фахівців [6, 61–62, 74–80, 101–107, 128–131, 140–145] дозволяє сформулювати такі основні проблеми створення системи ЕЦП на об'єктах інформаційної діяльності.

1. Регулювання взаємовідносин між учасниками процесів надання ЕЦП і сертифікації ключів.

2. Обґрунтування вибору архітектури системи ЕЦП з урахуванням завдань, що вирішуються на рівні відомства, державної установи, організацій, суспільних організацій (системний рівень).

3. Визначення та закріплення основних функціональних вимог до системи ЕЦП та сертифікації ключів (процедурно-функціональний рівень).

4. Визначення функціональної структури системи ЕЦП, порядку взаємодій із центрами сертифікації ключів з метою забезпечення необхідної якості надання послуг (функціонально-технічний рівень).

5. Обґрунтування вибору та ефективної реалізації апаратних засобів ЕЦП, у тому числі засобів криптографічного захисту (технічний рівень).

Аналіз указаних проблемних завдань дає змогу зробити висновок, що проектування та впровадження системи ЕЦП в рамках об'єкта інформаційної діяльності є окремою конструкторською та інженерною задачею.

Важливим етапом проектування системи ЕЦП є первинне обстеження об'єкта інформаційної діяльності, метою якого є збір та аналіз даних про інформацію та інші ресурси інформаційно-телекомунікаційних систем, існуючу систему забезпечення безпеки інформації, аналіз вимог щодо необхідності забезпечення цілісності, достовірності електронних документів з метою прийняття та обґрунтування рішення щодо впровадження системи ЕЦП, визначення стратегії, основних підходів використання послуг ЕЦП, встановлення правил застосування сертифікатів тощо.

Як правило, основними задачами обстеження є:

1) аналіз існуючої організаційно-штатної структури забезпечення безпеки інформації організації чи відомства;

2) аналіз чинних розпорядчих документів організації з питань організації електронного документообігу та захисту інформації в цілому;

3) визначення та класифікація інформаційних ресурсів організації, що особливо потребують забезпечення цілісності та справжності;

4) первинний аналіз ІТС (перш за все систем електронних документів та електронного документообігу) організації та визначення вимог щодо можливості використання надійних засобів ЕЦП;

5) розробка моделі загроз та висування організаційних вимог щодо забезпечення цілісності інформації.

Досягнення мети та вирішення сформульованих задач можливе на основі визначеної методики, яка об'єднує зміст і порядок проведення обстеження об'єкта інформаційної діяльності.

Основними нормативно-правовими актами для створення системи ЕЦП в Україні є такі:

1) Закон України «Про електронний цифровий підпис» від 22.05.2003 № 852-IX;

2) Закон України «Про електронні документи та електронний документообіг» від 22.05.2003 №851-IV;

3) Директива 1999/93/ЄС Європейського парламенту та Ради від 13 грудня 1999 року «Про систему електронних підписів, що застосовується в межах Співтовариства»;

4) Постанова КМУ від 26.05.2004 № 680 «Порядок засвідчення наявності электронного документа (електронних даних) на певний момент часу»;

5) Постанова КМУ від 13.06.2004 № 903 «Порядок акредитації центру сертифікації ключів»;

6) Постанова КМУ від 28.10.2004 № 1451 «Положення про центральний засвідчувальний орган»;

7) Постанова КМУ від 28.10.2004 № 1452 «Порядок застосування електронного цифрового підпису органами місцевого самоврядування, підприємствами, установами та організаціями державної форми власності»;

8) Постанова КМУ від 28.10.2004 № 1453 «Типовий порядок здійснення електронного документообігу в органах виконавчої влади»;

9) Постанова КМУ від 28.10.2004 № 1454 «Порядок обов'язкової передачі документованої інформації»;

10) ISO/IEC 9594-8:2005 (3d edition) Information technology – Open Systems Interconnection – The Directory: Authentication framework;

11) ДСТУ ISO/IEC 9594-8:2006 Інформаційні технології – Взаємодія відкритих систем – Каталог. Частина 8. Основні положення щодо сертифікації відкритих ключів та атрибутів. Наказ Держспоживстандарту від 26.12.2006 № 372;

12) ДСТУ ISO/IEC 14888-3 Інформаційні технології. Методи захисту. Цифрові підписи з додатком;

13) ДСТУ 4145-2002 Інформаційні технології. Криптографічний захист інформації. Цифровий підпис, що ґрунтується на еліптичних кривих. Формування та перевірка;

14) ГОСТ 34.10 Информационная технология. Криптографическая защита информации. Процессы формирования и проверки электронной цифровой подписи;

15) PKCS #1 RSA Cryptography;

16) ДСТУ ISO/IEC 10118 Інформаційні технології. Методи захисту. Геш-функції;

17) ГОСТ 34.11-94 Информационная технология. Криптографическая защита информации. Функция хэширования;

18) Правила посиленої сертифікації, затверджені наказом ДСТСЗІ СБ України від 13.01.2005 № 3 та зареєстровані в Міністерстві юстиції України за №104/10384 від 27.01.2005 та в редакції наказу Департаменту спеціальних телекомунікаційних систем і захисту інформації Служби безпеки України від 10.05.2006 № 50;

19) Положення про порядок розроблення, виробництва та експлуатації засобів криптографічного захисту конфіденційної та відкритої інформації з використанням електронного цифрового підпису. Затверджено наказом Адміністрації Державної служби спеціального зв'язку та захисту інформації України від 20.07.2007 № 862/14129.

9.2. ВИМОГИ ДО СИСТЕМИ ЕЦП УКРАЇНИ

Досвід технологічно розвинених держав свідчить, що основні завдання мають вирішуватись на ряді рівнів, перш за все на законодавчому, загальносистемному, процедурно-функціональному, функціонально-технічному та програмно-технічному рівнях [5, 51, 63–73, 81–83, 146–157, 220–234]. Аналіз ряду джерел [6, 61–62, 74–80, 101–107, 128–131, 140–145, 220–232] дозволив обґрунтувати та визначити сутність найбільш важливих вимог до системи ЕЦП України.

На законодавчому та нормативно-правовому рівнях важливим є врегулювання взаємовідносин замовників, розробників, постачальників, довірчих сторін і користувачів, тобто сторін, що беруть участь у функціонуванні системи ЕЦП. Важливим завданням є підготовка, перепідготовка та атестування обслуговуючого персоналу тощо.

9.2.1. Загальні вимоги до системи ЕЦП України

На загальносистемному рівні важливо обґрунтувати та висунути вимоги щодо загальної архітектури ІВК, складу основних об'єктів і суб'єктів ІВК, їх взаємодії з урахуванням завдань, що розв'язуються на національному рівні, рівні державних органів влади, міністерств і відомств, державних установ і закладів, державних і приватних підприємств, громадських організацій та об'єднань, окремих громадян тощо.

На процедурно-функціональному рівні мають бути заданими:
– основні функціональні вимоги до системи сертифікації;
– загальні функціональні вимоги до системи ЕЦП;
– вимоги до генерування та розподілення ключів;
– вимоги до адміністраторів реєстрації та сертифікації;
– вимоги до довідника (реєстру) сертифікатів;
– вимоги до сертифікатів та до управління сертифікатами;
– вимоги до користувачів (власників) сертифікатів тощо.
На функціонально-технічному рівні мають бути задані [5, 6, 14]:
– основні вимоги та функціональна структура ЦЗО, ЗЦ, АЦСК, ЦСК;
– вимоги безпеки ЦЗО, ЗЦ, АЦСК, ЦСК;
– вимоги доступності (надійності) з необхідним рівнем гарантій;
– основні вимоги до обслуговуючого персоналу;
– вимоги спостережливості та неспростовності тощо.
На програмно-технічному рівні мають бути заданими:
– вимоги до операційних середовищ, апаратних та апаратно-програмних засобів;
– вимоги до криптографічних примітивів;
– вимоги до методів і засобів генерування ключів;
– вимоги до парольних систем;
– вимоги до ключової інформації тощо.

9.2.2. Вимоги до системи ЕЦП України

Основні вимоги до системи ЕЦП України наведені в «Правилах посиленої сертифікації», що розроблені на виконання постанови Кабінету Міністрів України від 13 липня 2004 року № 903 «Про затвердження Порядку акредитації центру сертифікації ключів» та визначають організаційні, технічні й технологічні вимоги до акредитованих центрів сертифікації ключів (АЦСК) під час обслуговування ними посилених сертифікатів відкритих ключів (далі – сертифікат) та забезпечення їх використання.

Сертифікати, що сформовані відповідно до вимог політики сертифікації, повинні використовуватися для підтримки електронного цифрового підпису, який задовольняє вимогам щодо підпису, що застосовується до даних в електронній формі, у такий самий спосіб, як і власноручні підписи задовольняють вимогам щодо документа на папері.

Акредитований центр повинен зобов'язати заявника виконувати такі основні вимоги [6]:

а) надавати повну та дійсну інформацію під час реєстрації, необхідну для формування сертифіката;

б) використовувати особистий ключ виключно для ЕЦП, а також додержуватися інших вимог щодо його використання, визначених акредитованим центром;

в) зберігати особистий ключ у таємниці, не допускати використання особистого ключа іншими особами;

г) використовувати надійні засоби ЕЦП для генерації особистих та відкритих ключів, формування та перевірки ЕЦП;

д) негайно інформувати центральний засвідчувальний центр про події, що трапилися до закінчення строку чинності сертифіката, а саме:

– втрату або компрометацію особистого ключа;

– втрату контролю щодо особистого ключа через компрометацію пароля, коду доступу до нього тощо;

– виявлену неточність або зміну даних, зазначених у сертифікаті;

– не використовувати особистий ключ у разі його компрометації.

Акредитований центр повинен мати Регламент роботи, що визначає порядок і процедури обслуговування сертифікатів підписувачів відповідно до вимог, визначених у Правилах посиленої сертифікації.

У Регламентах роботи мають бути визначені [6, 74–77]:

а) загальні положення (ідентифікаційні дані акредитованого центру – повне найменування, код за ЄДРПОУ, місцезнаходження, номери телефонів, електронна адреса електронного інформаційного ресурсу);

б) перелік суб'єктів, задіяних в обслуговуванні й використанні сертифікатів та їх функції;

в) сфера використання сертифіката, у тому числі:

– перелік сфер і додатків, у яких дозволяється використання сертифікатів, сформованих акредитованим центром;

– обмеження щодо використання сертифікатів, сформованих акредитованим центром;

г) порядок розповсюдження (публікації) інформації акредитованим центром, у тому числі:

– перелік інформації, що публікується акредитованим центром на електронному інформаційному ресурсі;

– час і порядок публікації сертифікатів і списків відкликаних сертифікатів;

д) порядок ідентифікації та автентифікації, у тому числі:

– механізми підтвердження володіння підписувачем особистим ключем, якому відповідний відкритий ключ надається для сертифікації;

– умови встановлення юридичної особи (представника юридичної особи) або фізичної особи – підписувача (інформація, що надається заявником під час реєстрації, види документів, на підставі яких встановлюється підписувач, необхідність особистої присутності підписувача в акредитованому центрі тощо);

– механізми автентифікації для підписувачів, які мають чинний сертифікат, сформований в акредитованому центрі;

– механізми автентифікації під час звернення до акредитованого центру щодо відкликання (блокування й скасування) та поновлення сертифіката;

е) умови, процедури та механізми, що пов'язані з формуванням, блокуванням, скасуванням і використанням сертифіката, у тому числі:

– процес подання запиту на сертифікацію (перелік суб'єктів, уповноважених здійснювати запит на сертифікацію, порядок подачі та оброблення запиту на сертифікацію, строки оброблення запиту на сертифікат тощо);

– надання сформованого сертифіката підписувачу та визнання сертифіката його власником;

– публікація сформованого сертифіката акредитованим центром;

– використання сертифіката та особистого ключа (відповідальність підписувача – власника сертифіката під час використання особистого ключа та сертифіката, відповідальність користувачів під час використання сертифіката);

– процедура подачі запиту на сертифікацію для підписувачів, які мають чинний сертифікат ключа, сформований акредитованим центром;

– скасування (блокування, поновлення) сертифіката (обставини скасування, блокування, поновлення) сертифіката;

– перелік суб'єктів, уповноважених здійснювати запит на скасування (блокування та поновлення) сертифіката;

– процедура подання запиту на скасування (блокування, поновлення) сертифіката;

– час оброблення запиту на скасування (блокування, поновлення) сертифіката;

– частота формування списку відкликаних сертифікатів та строки його дії;

– можливість та умови надання інформації про статус сертифіката в режимі реального часу);

– закінчення строку чинності сертифіката підписувача;

ж) управління та операційний контроль:

– фізичне середовище (опис спеціального приміщення, механізми контролю доступу до нього);

– процедурний контроль (перелік посад безпосередньо задіяних в обслуговуванні сертифікатів, їх функції та відповідальність з урахуванням режиму роботи акредитованого центру);

– ведення журналів аудиту автоматизованої системи акредитованого центру (типи подій, що фіксуються в журналі аудиту, частота перегляду, строки зберігання журналів аудиту, захист та резервне копіювання журналів аудиту, перелік посад, що можуть здійснювати перегляд журналів аудиту);

– ведення архівів (типи документів і даних, що підлягають архівуванню, строки зберігання архівів, механізми та порядок зберігання й захисту архівів);

з) управління ключами:

– генерація ключів (процес, порядок і умови генерації ключів акредитованого центру та підписувачів);

– процедури надання особистого ключа його власнику після генерації акредитованим центром;

– механізм надання відкритого ключа акредитованому центру для сертифікації;

и) забезпечення захисту особистого ключа:

– порядок захисту та доступу до особистого ключа акредитованого центру;

– резервне копіювання особистого ключа акредитованого центру, порядок та умови збереження, доступу та використання резервної копії.

Регламент повинен розроблятися до початку проведення процедури акредитації центру сертифікації ключів та затверджуватися керівником центру після його погодження з контролюючим органом. Після затвердження Регламенту роботи один його примірник надсилається до контролюючого органу. Акредитований центр через електронний інформаційний ресурс або в інший спосіб повинен забезпечувати ознайомлення користувачів з положеннями Регламенту роботи або з іншими документами, що підтверджують відповідність його діяльності політиці сертифікації, визначеної у Правилах.

Управління ключами в акредитованому центрі.
Генерація ключів акредитованого центру

Генерація особистого ключа акредитованого центру повинна здійснюватись у спеціальному приміщенні за участю або під контролем не менше двох визначених осіб із обслуговуючого персоналу. Генерація ключів акредитованого центру здійснюється за допомогою надійних засобів ЕЦП. Усі події, пов'язані з генерацією, використанням та знищенням особистого ключа акредитованого центру, повинні протоколюватися.

Зберігання, резервування та відновлення особистого ключа акредитованого центру

Особистий ключ акредитованого центру повинен розміщуватися:

– на захищеному носії у складі програмно-апаратного або апаратного засобу криптографічного захисту інформації (далі – КЗІ), яким здійснювалася генерація ключів згідно з Правилами;

– на незйомному носії (пристрої) зі складу програмно-технічного комплексу або зйомному носії (пристрої). Порядок зберігання та доступу до особистого ключа в такому випадку погоджується з Департаментом спеціальних телекомунікаційних систем та захисту інформації Служби безпеки України.

У разі здійснення резервування особистого ключа акредитованого центру особистий ключ повинен бути перенесений на зовнішній носій (пристрій) у захищеному вигляді, що забезпечує його цілісність і конфіденційність. Резервування, зберігання та відновлення особистого ключа повинно здійснюватися в спеціальному приміщенні. Резервування та відновлення здійснюється за участю або під контролем не менше двох визначених осіб із числа обслуговуючого персоналу. Умови забезпечення захисту резервної копії особистого ключа акредитованого центру під час його зберігання повинні бути не нижче, ніж умови забезпечення захисту особистого ключа, що знаходиться у використанні. У разі якщо ключ зберігається у призначеному для цього програмно-апаратному або апаратному засобі КЗІ, технологія зберігання повинна забезпечити неможливість доступу до нього ззовні.

Використання особистого ключа акредитованого центру

Особистий ключ акредитованого центру може використовуватися тільки для формування сертифікатів (накладання ЕЦП на сертифікат) та інформації про статус сертифіката. Особистий ключ акредитованого центру може використовуватися тільки в засобах КЗІ, які мають бути розташовані в спеціальному приміщенні.

Строк чинності особистого ключа акредитованого центру

Особистий ключ акредитованого центру може бути чинним не більше ніж п'ять років. Після закінчення терміну дії особистого ключа акредитованого центру особистий ключ та всі його резервні копії знищуються способом, що не дозволяє їх відновлення.

Надання допомоги щодо генерації ключів підписувачам

У разі генерації ключів підписувачам акредитований центр повинен вжити заходів для забезпечення конфіденційності під час генерації ключів.

У разі передачі акредитованим центром особистого ключа підписувачу через заявника повинна бути забезпечена конфіденційність і цілісність особистого ключа. Зберігання особистих ключів підписувачів та ознайомлення з ними в акредитованому центрі забороняються. Генерація ключів акредитованим центром підписувачам повинна здійснюватися за допомогою надійних засобів ЕЦП.

Обслуговування сертифікатів

Обслуговування акредитованим центром сертифікатів передбачає:
– реєстрацію;
– сертифікацію;
– розповсюдження;
– управління статусом сертифіката;
– розповсюдження інформації про статус сертифіката.
Додатково акредитований центр може надавати засоби ЕЦП.

Повторне формування сертифіката

При повторному формуванні сертифіката акредитований центр повинен здійснити перевірку щодо того, чи дійсна інформація, яка надавалася раніше заявником під час реєстрації. Якщо виникає необхідність зміни даних, зазначених у сертифікаті, акредитований центр може здійснити переформування сертифіката підписувачу із використанням попередньо засвідченого відкритого ключа підписувача у разі, якщо відповідний йому особистий ключ не був скомпрометований. При цьому не повинні бути порушені вимоги пункту Правил, а час чинності особистого ключа та відповідного йому відкритого ключа не може перевищувати двох років.

Формування сертифіката

Формування сертифіката підписувачу здійснюється акредитованим центром на підставі даних, отриманих від заявника під час реєстрації. Формат сертифіката, що відповідає вимогам Закону України «Про електронний цифровий підпис», визначається відповідними технічними специфікаціями форматів представлення базових об'єктів національної системи ЕЦП. У разі якщо центр сертифікації ключів акредитується засвідчувальним центром та надає послуги ЕЦП в межах інформаційної системи з обмеженим колом користувачів, що визначене власником інформаційної системи або відповідними угодами користувачів цієї системи, такий акредитований центр може використовувати формат сертифіката, визначений засвідчувальним центром. Акредитований центр повинен забезпечити унікальність розпізнавального імені підписувача та реєстраційного номера сертифіката в межах акредитованого центру. Для фізичної особи обов'язковими реквізитами розпізнавального імені є прізвище, ім'я та по батькові, а для юридичної особи – повна назва юридичної особи відповідно до статуту (положення) та ідентифікаційний код за ЄДРПОУ. Додаткові дані підписувача (належність до певної організації, посада тощо) вносяться у сертифікат за бажанням заявника або відповідно до вимог нормативно-правових актів, що встановлюють особливості застосування ЕЦП у відповідній сфері.

В акредитованому центрі має бути передбачена можливість резервування всіх сформованих ним сертифікатів. Усі події, що пов'язані із формуванням,

переформуванням, блокуванням, поновленням і скасуванням сертифікатів, виданих акредитованим центром, повинні протоколюватися в акредитованому центрі із забезпеченням захисту протоколів від несанкціонованого доступу.

Розповсюдження умов обслуговування та використання сертифіката

Акредитований центр повинен надати вільний доступ користувачам до інформації щодо умов, пов'язаних з використанням сертифіката, зокрема:

– положень політики сертифікації, визначеної у цих Правилах;

– обмежень при використанні сертифіката;

– зобов'язань і підстав відповідальності підписувачів стосовно використання сертифіката, у тому числі щодо використання надійних засобів ЕЦП;

– інформації щодо порядку перевірки чинності сертифіката, у тому числі умов перевірки статусу сертифіката;

– строків зберігання акредитованим центром даних про підписувачів, що були отримані ним під час реєстрації;

– порядку розв'язання суперечок;

– законодавства у сфері ЕЦП;

– підстав відповідальності акредитованого центру.

Зазначена інформація може надаватися через електронний інформаційний ресурс або в інший спосіб, що дає можливість з нею ознайомитися.

Розповсюдження сертифікатів

Після формування сертифікат повинен бути доступний заявнику та/або підписувачу, для якого цей сертифікат був сформований. Доступ до сформованого сертифіката для користувачів надається в разі згоди на це заявника, якщо для державних органів інше не передбачене правилами їх систем електронного документообігу. Дані, що визначені у Правилах, повинні бути вільно доступними для користувачів цілодобово.

Блокування та скасування сертифікатів

Акредитований центр повинен визначити в Регламенті роботи умови та процедури відкликання сертифіката, зокрема:

– хто може звернутися до акредитованого центру щодо блокування або скасування сертифіката;

– порядок звернення до акредитованого центру щодо блокування або скасування сертифіката;

– умови підтвердження звернення щодо скасування або блокування сертифіката;

– причини, за якими сертифікат може бути заблокований;

– механізми (методи), що використовуються акредитованим центром для розповсюдження інформації про статус сертифіката;

– максимальний час між отриманням звернення щодо скасування або блокування сертифіката та зміною його статусу, інформація про який доступна користувачам.

Особа, яка звертається до акредитованого центру щодо скасування сертифіката, повинна бути встановлена, а також перевірено законність такого звернення. Вимоги щодо підтвердження запиту на скасування сертифіката встановлюються

акредитованим центром. Підписувач, сертифікат якого був заблокований або скасований, повинен бути проінформований про зміну статусу сертифіката. Скасований сертифікат не може бути в подальшому поновлений.

У разі якщо для розповсюдження інформації про статус сертифіката акредитованим центром використовується механізм списку відкликаних сертифікатів, мають бути забезпечені такі умови:

– кожний список відкликаних сертифікатів повинен містити час видання наступного списку, якщо інше не передбачено Регламентом роботи;

– новий список відкликаних сертифікатів може бути опублікований до визначеного часу видання наступного списку;

– список відкликаних сертифікатів повинен бути підписаний за допомогою особистого ключа акредитованого центру.

Формат списку відкликаних сертифікатів

Визначається відповідними технічними специфікаціями форматів представлення базових об'єктів національної системи ЕЦП. Управління статусом сертифіката та розповсюдження інформації про статус сертифіката повинні бути вільно доступні цілодобово. Звернення щодо скасування сертифікатів фіксуються та зберігаються в акредитованому центрі. Акредитований центр повинен забезпечити цілісність і автентичність інформації щодо статусу сертифікатів. Час, що використовується в процесі обслуговування сертифікатів для надання послуг, повинен бути синхронізований із Всесвітнім координованим часом з точністю до однієї секунди.

Забезпечення безпеки інформаційних ресурсів в акредитованому центрі

Загальні вимоги

Безпека інформаційних ресурсів в акредитованому центрі досягається шляхом впровадження організаційних, інженерно-технічних заходів, засобів і методів технічного та криптографічного захисту інформації комплексної системи захисту інформації (далі – КСЗІ), спрямованих на забезпечення захисту інформації під час обслуговування сертифікатів ключів. КСЗІ автоматизованої системи акредитованого центру повинна мати атестат відповідності нормативним документам із захисту інформації. Засоби КЗІ акредитованого центру повинні мати позитивний експертний висновок за результатами державної експертизи у сфері КЗІ. Захищений носій також повинен мати сертифікат відповідності або позитивний експертний висновок на відповідність вимогам технічного захисту інформації.

Вимоги до обслуговуючого персоналу

Обслуговуючий персонал акредитованого центру повинен мати відповідні знання, досвід і навички, необхідні для забезпечення надання послуг ЕЦП. Функції та відповідальність обслуговуючого персоналу, діяльність якого безпосередньо пов'язана з безпекою функціонування акредитованого центру відповідно до політики безпеки акредитованого центру, повинні бути передбачені їх посадовими обов'язками (посадовими інструкціями).

В акредитованому центрі мають бути визначені такі посади обслуговуючого персоналу, діяльність яких безпосередньо пов'язана з безпечним функціонуванням акредитованого центру:

– адміністратор реєстрації, який відповідає за встановлення фізичних і юридичних осіб під час формування, блокування, поновлення та скасування сертифіката;

– адміністратор сертифікації, який відповідає за формування сертифікатів, списків відкликаних сертифікатів, збереження та використання особистого ключа акредитованого центру;

– адміністратор безпеки, який відповідає за належне функціонування КСЗІ та входить до складу служби захисту інформації акредитованого центру;

– системний адміністратор, який відповідає за функціонування програмно-технічного комплексу.

Забороняється суміщення посади адміністратора безпеки з іншими посадами.

Забезпечення безпеки фізичного середовища

Фізичний доступ до обладнання програмно-технічного комплексу, що забезпечує сертифікацію, управління статусом сертифіката, генерацію ключів акредитованого центру, повинен бути обмежений і надаватися тільки визначеному колу осіб із числа обслуговуючого персоналу. В акредитованому центрі повинно бути вжито запобіжних заходів щодо недопущення крадіжки, втрати та ушкодження обладнання, крадіжки та знищення (руйнування) інформації або інших дій, що можуть призвести до виведення акредитованого центру зі штатного режиму роботи. Обладнання програмно-технічного комплексу, що забезпечує формування сертифіката, управління статусом сертифіката, генерацію ключів акредитованого центру, повинно розміщуватися в спеціальному приміщенні акредитованого центру, що забезпечує фізичний захист від несанкціонованого доступу до зазначених систем і даних, що ними обробляються.

Управління доступом до інформаційних ресурсів акредитованого центру

В акредитованому центрі повинен бути передбачений захист внутрішньої обчислювальної мережі від втручання з боку зовнішньої мережі (глобальних мереж), що є доступною для користувачів. Дані про підписувача, що надаються під час реєстрації, мають бути захищені в разі їх передавання зовнішніми комп'ютерними мережами. В акредитованому центрі повинно бути реалізовано адміністрування з метою розмежування доступу обслуговуючого персоналу до ресурсів системи та надання функцій тільки згідно з авторизацією обслуговуючого персоналу (можливості виконувати тільки ті функції, що доступні та асоційовані з їх ролями). Обслуговуючий персонал має бути успішно ідентифікований та автентифікований перед початком виконання процедур, пов'язаних із формуванням сертифіката або зміною його статусу. Усі дії обслуговуючого персоналу, пов'язані з генерацією ключів, формуванням сертифіката чи зміною його статусу, повинні протоколюватися із забезпеченням захисту протоколів від несанкціонованого доступу. Резервні копії сертифікатів і журналів аудиту програмно-технічного комплексу повинні зберігатися в окремому приміщенні із забезпеченням їх захисту від несанкціонованого доступу. Програмно-технічний комплекс повинен забезпечувати реєстрацію дій обслуговуючого персоналу. Журнали аудиту системи повинні мати захист від несанкціонованого доступу, модифікації або знищення (руйнування).

Програмно-технічний комплекс повинен забезпечити реєстрацію таких подій:

– спроби створення, знищення, встановлення пароля, зміни прав доступу, системних привілеїв тощо у програмно-технічному комплексі;

– заміни ключів;

– формування, переформування, блокування, скасування та поновлення посилених сертифікатів ключів, а також формування списків скасованих сертифікатів;

– спроби несанкціонованого доступу до програмно-технічного комплексу;

– надання доступу до програмно-технічного комплексу персоналу акредитованого центру;

– збої в роботі програмно-технічного комплексу.

Усі записи в журналах аудиту в електронній або паперовій формі повинні містити дату та час події, а також ідентифікувати суб'єкта, що ініціював цю подію.

9.3. ІНФОРМАЦІЙНА СТРУКТУРА СИСТЕМИ ЕЦП УКРАЇНИ

Інфраструктуру системи ЕЦП в Україні прийнято будувати за ієрархічним принципом. Вона значною мірою перш за все схожа на ІВК Уряду Канади, оскільки остання розроблена на десятиріччя раніше, та значною мірою схожа на систему Російської Федерації, яка створюється паралельно з системою ЕЦП України.

На рис. 9.1 наведено узагальнену схему інформаційної структури відкритих ключів України. Основними структурними елементами системи ЕЦП України є Центральний засвідчувальний орган (ЦЗО), засвідчувальні центри (ЗЦ) Центральних органів виконавчої влади, акредитовані центри сертифікації ключів (АЦСК), центри сертифікації ключів (ЦСК), відокремлені пункти реєстрації ключів, заявники – юридичні та фізичні особи (користувачі), Контролюючий орган.

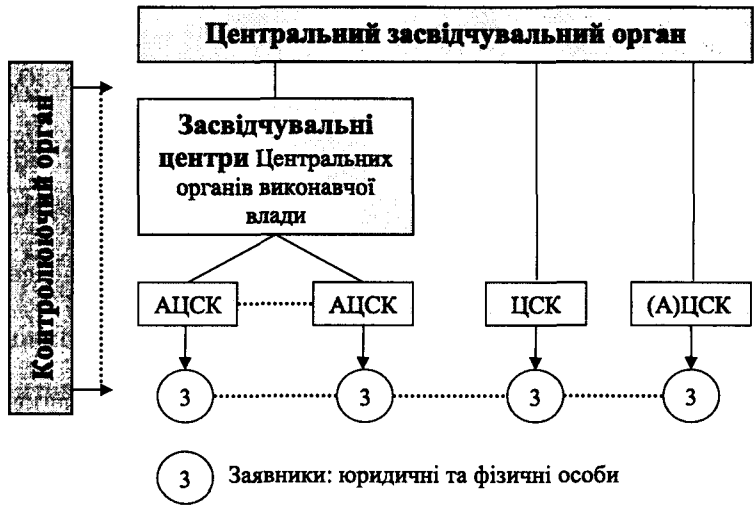

Рис. 9.1. Узагальнена схема інформаційної структури відкритих ключів України

ЦЗО у національній системі електронного цифрового підпису України є кореневим центром сертифікації відкритих ключів, основними завданнями якого є обслуговування посилених сертифікатів ключів центрів в Україні, акредитація центрів сертифікації ключів та засвідчувальних центрів відповідно до законодавства України.

На міждержавному рівні ЦЗО є мостовим центром перехресної сертифікації ключів відповідної ІВК з мостовими центрами інших держав і союзів, основними завданнями якого є обслуговування перехресних сертифікатів ключів мостового центру в Україні, акредитація мостового центру та забезпечення дотримання ним Політики перехресної сертифікації з визначеним рівнем гарантій.

ЦЗО відповідно до покладених на нього завдань щодо внутрішньодержавної системи ЕЦП [2, 6, 76]:

– здійснює акредитацію центрів, видачу, переоформлення й анулювання відповідних свідоцтв;

– формує і видає центрам сертифікати ключів;

– проводить реєстрацію центрів;

– блокує, скасовує та поновлює сертифікати ключів центрів у випадках, передбачених Законом [2, 6];

– веде Реєстр суб'єктів, які надають послуги, пов'язані з електронним цифровим підписом;

– веде електронні реєстри сертифікатів ключів центрів, у тому числі блокованих і скасованих;

– зберігає сертифікати ключів центрів;

– забезпечує цілодобово доступ до сертифікатів ключів центрів та їх електронних реєстрів через загальнодоступні телекомунікаційні мережі;

– надає центрам консультації з питань, пов'язаних з використанням електронного цифрового підпису;

– забезпечує діяльність постійно діючої комісії з питань акредитації (далі – ПДКА) центрів, яка утворюється при ЦЗО. Склад та функції ПДКА затверджуються наказом Державного комітету інформатизації України;

– приймає на зберігання сертифікати ключів, їх реєстри та документовану інформацію, яка підлягає обов'язковій передачі від центрів до ЦЗО в разі припинення їх діяльності;

– розглядає заяви і скарги щодо неналежного функціонування центрів та подає відповідні пропозиції контролюючому органу;

– повідомляє контролюючий орган про обставини, які перешкоджають діяльності ЦЗО.

На міждержавному рівні ЦЗО є мостовим центром перехресної сертифікації ІВК з мостовими центрами інших держав і союзів.

ЦЗО відповідно до покладених на нього завдань щодо зовнішньої міждержавної ІВК [2, 6, 76]:

– здійснює акредитацію мостового центру перехресної сертифікації ключів, видачу, переоформлення та анулювання відповідних свідоцтв;

– визначає та затверджує політики перехресної сертифікації та рівні гарантій мостового центру ЦЗО, узгоджуючи їх з відповідними політиками та рівнями гарантій мостового центру, з яким здійснюється перехресна сертифікація;

– у відповідності з рівнем гарантій, що визначені політикою перехресної сертифікації, забезпечує генерування асиметричних ключових пар з використанням відповідного рівня гарантій модуля криптографічного захисту інформації;

– проводить реєстрацію об'єктів, що є користувачами мостового центру перехресної сертифікації, з обов'язковою їх ідентифікацією та автентифікацією;

– затверджує угоди на використання об'єктами послуг перехресної сертифікації відкритих ключів з регламентацією їх обов'язків і відповідальності за взаємодію;

– формує та видає користувачам і центрам сертифікати відкритих ключів у системі перехресної сертифікації;

– засобом відображення політик контролює інтероперабельність перехресно сертифікованих об'єктів;

– забезпечує перекодування та модифікацію перехресно сертифікованих відкритих ключів об'єктів у відповідності з діючими політиками;

– блокує, скасовує та поновлює перехресні сертифікати відкритих ключів центрів і сертифікати ключів користувачів у випадках, передбачених Законом та відповідно до взаємно визнаної центрами політики перехресної сертифікації;

– веде Реєстр суб'єктів, які користуються послугами перехресної сертифікації відкритих ключів, що зв'язані з ІВК;

– зберігає сертифікати відкритих ключів центрів та користувачів, що є об'єктами перехресної сертифікації;

– надає центрам та користувачам перехресної сертифікації консультації з питань, пов'язаних з використанням ІВК;

– забезпечує захист ідентифікаційної та службової інформації з питань перехресної сертифікації користувачів і мостових центрів;

– забезпечує діяльність постійно діючої комісії з питань Політики перехресної сертифікації (ППС) та надання центрам і користувачам послуг перехресної сертифікації, яка утворюється при ЦЗО;

– приймає на зберігання перехресні сертифікати ключів, їх реєстри та документовану інформацію, яка підлягає обов'язковій передачі від мостового центру ЦЗО на зберігання в разі припинення їх діяльності;

– розглядає заяви і скарги щодо неналежного функціонування мостового центру та подає відповідні пропозиції контролюючому органу;

– повідомляє контролюючий орган про обставини, які перешкоджають діяльності ЦЗО щодо надання центрам і користувачам послуг перехресної сертифікації.

Акредитований центр сертифікації ключів (АЦСК) здійснює свою діяльність у сфері електронного документообігу, застосування ЕЦП органами державної влади, органами місцевого самоврядування, підприємствами, установами й організаціями всіх форм власності, іншими суб'єктами господарської діяльності та фізичними особами [2, 6, 76].

Послуги ЕЦП, що надаються Центром

Під послугами електронного цифрового підпису розуміють надання в користування засобів електронного цифрового підпису, допомогу при генерації відкритих та особистих ключів, обслуговування сертифікатів ключів (формування, розповсюдження, скасування, зберігання, блокування й поновлення), надання інформації щодо чинних, скасованих і блокованих сертифікатів ключів, послуги фіксування часу, консультації та інші послуги, визначені Законом України від 22.05.2003 № 852-IV «Про електронний цифровий підпис».

Перелік послуг ЕЦП, що надаються Центром [2, 6, 75]:

– обслуговування сертифікатів відкритих ключів (далі – сертифікатів) Абонентів, що включає:

– реєстрацію Абонентів;

– надання Абонентам засобів ЕЦП та шифрування даних, засобів генерації особистих і відкритих ключів;

– сертифікацію відкритих ключів Абонентів;

– розповсюдження сертифікатів;

– управління статусом сертифікатів та розповсюдження інформації про статус сертифікатів;

– надання послуг фіксування часу.

Окрім надання послуг ЕЦП, Центр надає консультаційні послуги за зверненням Абонентів.

Надання вищезазначених послуг здійснюється Центром у відповідності до цього Регламенту та на підставі укладених договорів.

Порядок застосування електронного цифрового підпису органами державної влади, органами місцевого самоврядування, підприємствами, установами й організаціями державної форми власності визначається Кабінетом Міністрів України.

Порядок застосування цифрового підпису в банківській діяльності визначається Національним банком України.

Відокремлені пункти реєстрації [2 , 6, 76]

Відокремлені пункти реєстрації заявників є відособленими підрозділами без правового статусу юридичної особи, що реалізують функції Центру з реєстрації Абонентів та їх подальшого обслуговування на відповідній території.

Відокремлені пункти діють на підставі Положення про відокремлений пункт та Регламенту АЦСК.

Відокремлені пункти уповноважені укладати договори про надання послуг ЕЦП.

Безпосереднє управління відокремленими пунктами здійснюється Центром сертифікації ключів.

Варіант структурної схеми АЦСК на прикладі Міністерства освіти та науки України наведений на рис. 9.2.

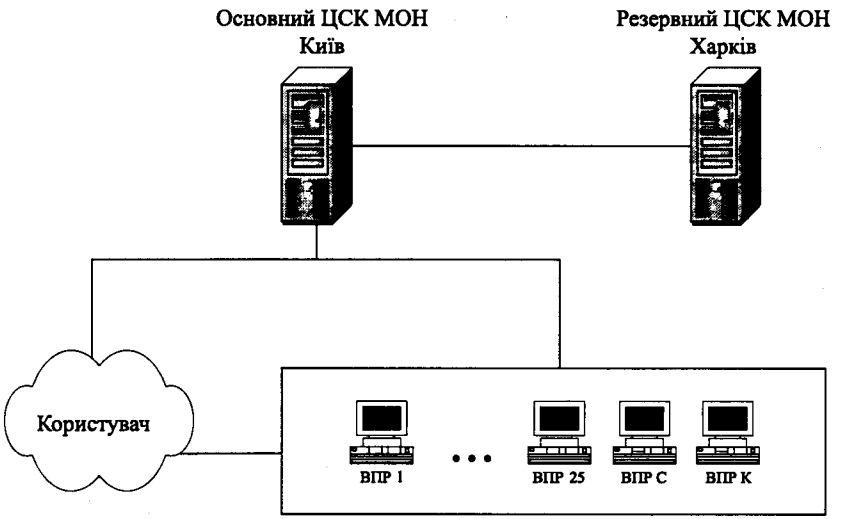

Рис. 9.2. Структурна схема АЦСК на прикладі Міністерства освіти та науки України

Абоненти (користувачі) ЕЦП

Абонент має право:

– своєчасно отримувати якісні послуги ЕЦП;

– одержувати сертифікат Центру;

– одержувати список відкликаних сертифікатів, сформований Центром;

– застосовувати сертифікат Центру для перевірки справжності ЕЦП сертифікатів, сформованих Центром;

– застосовувати список відкликаних сертифікатів, сформований Центром, для перевірки статусу власного сертифіката та сертифікатів інших Абонентів;

– сформувати відкриті й особисті ключі на своєму робочому місці з використанням надійного засобу ЕЦП;

– ознайомитись з інформацією щодо діяльності Центру та надання послуг ЕЦП;

– подавати заяви, скарги, претензії;

– вимагати скасування, блокування або поновлення свого сертифіката ключа;

– вимагати від Центру усунення порушень умов даного Регламенту та договору про надання послуг ЕЦП;

– вимагати від Центру виконання вимог конфіденційності;

– оскаржити дії чи бездіяльність Центру в судовому порядку.

Абонент зобов'язаний:

– ознайомитись та дотримуватись правил надання послуг ЕЦП;

– надавати під час реєстрації повну та дійсну інформацію, необхідну для формування сертифіката Абонента;

– зберігати в таємниці особистий ключ і вживати всіх можливих заходів для запобігання його втрати, розкриття, перекручування та несанкціонованого використання;

– не розголошувати та не повідомляти іншим особам пароль доступу до особистого ключа та ключову фразу для голосової автентифікації;

– використовувати особистий ключ виключно для мети, визначеної в сертифікаті, та додержуватися інших обмежень щодо використання сертифіката;

– використовувати надійні засоби ЕЦП для генерації особистих і відкритих ключів, формування та перевірки ЕЦП;

– негайно інформувати Центр про факти компрометації особистого ключа, виявлення неточностей або зміни даних у сертифікаті;

– не застосовувати особистий ключ, якщо стало відомо, що цей ключ використовується або використовувався раніше іншими особами;

– негайно інформувати Центр про наступні події, що трапилися до закінчення строку чинності сертифіката: компрометацію особистого ключа; компрометацію паролю захисту особистого ключа; виявлену неточність або зміни даних, зазначених у сертифікаті;

– не використовувати особистий ключ у разі його компрометації;

– не використовувати особистий ключ, відповідний до сертифіката, заява на скасування чи блокування якого подана до Центру, протягом часу з моменту подання заяви й до моменту офіційного повідомлення про скасування сертифіката;

– не використовувати особистий ключ, відповідний до сертифіката, що скасований або блокований.

Відповідальність сторін

У разі невиконання своїх обов'язків за визначеним Регламентом Центр або Абонент (Сторони), повинні в повному обсязі відшкодувати збитки, заподіяні іншій стороні, у порядку, встановленому чинним законодавством.

Сторони несуть відповідальність за дії своїх співробітників, а також інших осіб, які мають або мали доступ (незалежно від того, був цей доступ санкціонований Стороною чи виник з її провини) до апаратних засобів, програмного, інформаційного забезпечення, криптографічних ключів та інших засобів ЕЦП, як за свої особисті.

Сторони не відповідають за невиконання або неналежне виконання своїх обов'язків за даним Регламентом, а також за збитки, які виникли у зв'язку із цим, у випадках, якщо це є наслідком зустрічного невиконання або неналежного зустрічного виконання іншою Стороною своїх обов'язків.

Центр не несе відповідальності за майнову та моральну шкоду, що була спричинена Абоненту неналежною роботою програмного забезпечення Центру в разі, якщо неналежна робота програмного забезпечення була викликана «мережевими атаками», дією «вірусних програм» або іншим неякісним (неліцензованим) програмним забезпеченням Абонента.

Центр не несе відповідальності за майнову та моральну шкоду, що може бути спричинена Абоненту (або третім особам), та в разі невиконання або неналежного виконання Абонентом цього Регламенту та договору про надання послуг ЕЦП.

Центр не відповідає за невиконання або неналежне виконання своїх обов'язків за цим Регламентом, а також за збитки, що виникли у зв'язку із цим, у разі:

– якщо Центр обґрунтовано покладався на відомості, зазначені в заяві Абонента;

– підробки, підміни або іншого перекручування Абонентом або його уповноваженим представником відомостей, що містяться в заяві або в інших документах, наданих одній стороні від імені іншої сторони.

Центр відповідає за збитки при використанні особистого ключа та сертифіката Абонента тільки у випадку, якщо ці збитки виникли внаслідок компрометації особистого ключа Центру або внаслідок невідповідності відомостей у сертифікаті відомостям, зазначеним у заяві Абонента.

Виплата пені та відшкодування збитків не звільняє сторони від виконання своїх обов'язків за даним регламентом.

Відповідальність сторін, яка не врегульована положеннями даного Регламенту, регулюється чинним законодавством України.

Сторони звільняються від відповідальності за повне або часткове невиконання своїх зобов'язань, якщо таке невиконання сталося внаслідок настання форс-мажорних обставин, таких, як пожежа, повінь землетрус, інше стихійне лихо, військові дії, дія надзвичайного стану, блокада, громадські масові зворушення, страйки, аварії на транспорті, диверсії, розпорядження Державних органів влади, або за інших обставин, які не залежать від волі Сторін, за умови, що ці обставини безпосередньо впливають на виконання їх зобов'язань і їх неможливо було передбачити на момент укладання договору про надання послуг ЕЦП.

Сторона, що через зазначені вище обставини не може в повному обсязі виконувати свої зобов'язання, повинна в строк не більше п'яти днів письмово сповістити про це іншу Сторону, а в строк десяти днів надати відповідні документи, які це підтверджують.

Несвоєчасне (пізніше 5-ти днів) повідомлення про існування обставин форс-мажору позбавляє відповідну Сторону права посилатися на них для виправдання.

Достатнім доказом існування обставин форс-мажору є довідки компетентних органів влади.

У випадку, якщо вищезгадані обставини будуть діяти більше трьох місяців, кожна із Сторін може письмово сповістити іншу про повне або часткове припинення дії договору про надання послуг ЕЦП, що звільняє Сторони від взаємних зобов'язань, за винятком проведення взаєморозрахунків у частині вже виконаних Сторонами зобов'язань.

Порядок розв'язання спорів і вирішення конфліктних ситуацій

Будь-яка конфліктна ситуація вирішується шляхом переговорів з дотриманням претензійного порядку.

У разі виникнення непорозумінь щодо виконання умов цього Регламенту та договору про надання послуг ЕЦП, які не вирішено мирним шляхом, або інших спірних питань, Сторона, яка вважає, що її права порушуються, зобов'язана в місячний строк з моменту, коли вона дізналась або повинна була дізнатись про таке порушення, направити іншій Стороні обґрунтовану претензію.

Претензія, направлена з порушенням зазначеного строку, не розглядається.

Термін розгляду претензії – 10 (десять) робочих днів з моменту її одержання.

Усі спірні ситуації, за якими не досягнуто згоди в претензійному порядку, вирішуються в господарському або загальному суді.

Контролюючий орган

Функції контролюючого органу здійснює спеціально уповноважений центральний орган виконавчої влади у сфері криптографічного захисту інформації – Державна служба спеціального зв'язку та захисту інформації України [2]. Контролюючий орган перевіряє дотримання Закону ЦЗО, ЗЦ, АЦСК та ЦСК. У разі невиконання або неналежного виконання обов'язків і виявлення порушень вимог, встановлених законодавством для ЦЗО, ЗЦ, АЦСК та ЦСК, контролюючий орган дає розпорядження ЦЗО про негайне вжиття заходів, передбачених законом.

9.4. ВИМОГИ ДО СТРУКТУРИ ТА ПРИЗНАЧЕННЯ КОМПЛЕКСУ ТЕХНІЧНИХ ЗАСОБІВ ЦЕНТРУ

Структурна схема комплексу технічних засобів наведена на рис. 9.3. До складу комплексу повинні входити такі технічні засоби (варіант):

- РС (робоча станція) адміністратора безпеки;
- РС системного адміністратора;
- РС адміністратора реєстрації;
- РС адміністратора сертифікації;
- сервер ЦСК;
- комутатор;
- сервер взаємодії;
- міжмережевий екран (МЕ);
- РС генерації ключів користувачів;
- РС віддаленого адміністратора реєстрації.

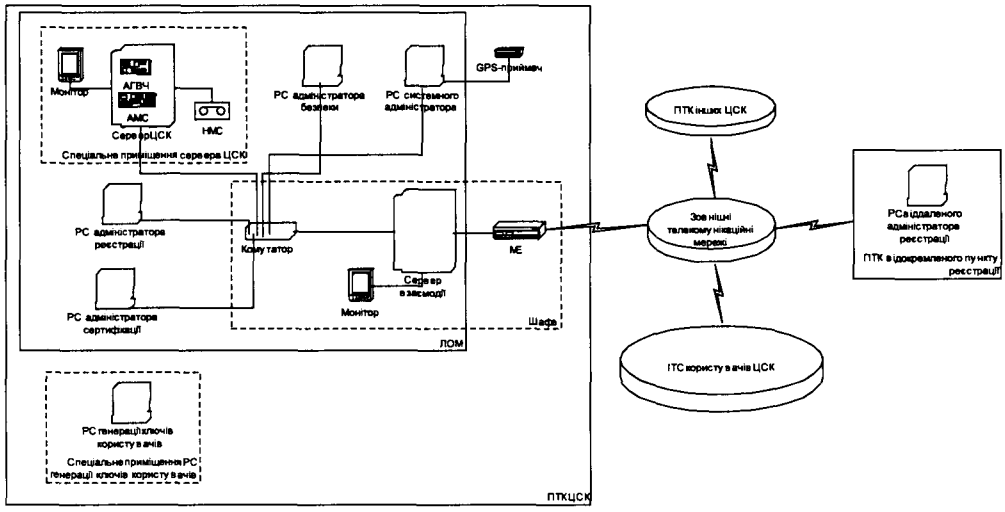

Рис. 9.3. Структурна схема комплексу технічних засобів

Вимоги до призначення РС адміністратора безпеки повинні бути визначені в окремому технічному завданні або технічному завданні на комплекс засобів захисту комплексу.

РС системного адміністратора повинна забезпечувати:

– налагодження параметрів технічних засобів комплексу та системного програмного забезпечення;

– діагностування роботи технічних засобів комплексу;

– моніторингу стану технічних засобів комплексу.

РС адміністратора реєстрації повинна забезпечувати:

– уведення реєстраційних даних користувачів до реєстру користувачів;

– зміни реєстраційних даних користувачів у реєстрі;

– видалення реєстраційних даних користувачів з реєстру;

– приймання та введення запитів користувачів на формування сертифікатів відкритих ключів на носіях інформації;

– приймання та введення запитів користувачів на скасування, блокування чи поновлення сертифікатів на носіях інформації;

– ініціювання скасування, блокування чи поновлення сертифікатів користувачів сервером ЦСК;

– генерації особистого та відкритого ключів адміністратора реєстрації;

– уведення та використання особистих ключів адміністратора реєстрації;

– формування та передачу запиту на формування сертифіката адміністратора реєстрації на сервер ЦСК;

– отримання, зберігання та використання сертифіката адміністратора реєстрації.

РС адміністратора сертифікації повинна забезпечувати:

– ініціювання публікації реєстру сертифікатів у загальнодоступні каталоги (LDAP-каталоги) та на інформаційному ресурсі ЦСК (web-сторінці) сервером ЦСК;

– розсилання реєстрів сертифікатів користувачам засобами електронної пошти;

– ініціювання формування списків відкликаних сертифікатів користувачів сервером ЦСК;

– ініціювання публікації списків відкликаних сертифікатів у загальнодоступні каталоги (LDAP-каталоги) та на інформаційному ресурсі ЦСК (web-сторінці) сервером ЦСК;

– оповіщення користувачів про зміну статусу сертифікатів засобами електронної пошти;

– ініціювання публікації сертифіката ЦСК у загальнодоступні каталоги (LDAP-каталоги) та на інформаційному ресурсі ЦСК (web-сторінці) сервером ЦСК.

Сервер ЦСК повинен забезпечувати:

– зберігання реєстру користувачів та забезпечення використання реєстраційних даних;

– резервне копіювання та архівування реєстру користувачів на носії інформації;

– приймання та реєстрацію запитів користувачів та адміністраторів реєстрації на формування сертифікатів користувачів;

– зберігання запитів на формування сертифікатів, отриманих від користувачів та адміністраторів реєстрації, у базі даних запитів;

– архівування бази даних запитів на формування сертифікатів;

– формування сертифікатів відкритих ключів користувачів;

– внесення сформованих сертифікатів у реєстр сертифікатів;

– зберігання реєстру сертифікатів;

– резервне копіювання реєстру сертифікатів;

– архівування реєстру сертифікатів;

– публікації реєстру сертифікатів у загальнодоступні каталоги (LDAP-каталоги) та на інформаційному ресурсі ЦСК (web-сторінці);

– розсилання реєстрів сертифікатів користувачам засобами електронної пошти;

– приймання та реєстрацію запитів користувачів і адміністраторів реєстрації на скасування, блокування чи поновлення сертифікатів;

– зберігання запитів на скасування, блокування чи поновлення сертифікатів, отриманих від користувачів та адміністраторів реєстрації, у базі даних запитів;

– архівування бази даних запитів на скасування, блокування чи поновлення сертифікатів;

– скасування, блокування чи поновлення сертифікатів на основі запитів;

– внесення інформації про поточний статус сертифіката до реєстру сертифікатів;

– формування списків відкликаних сертифікатів користувачів;

– публікації списків відкликаних сертифікатів у загальнодоступні каталоги (LDAP-каталоги) та на інформаційному ресурсі ЦСК (web-сторінці);

– приймання через сервер взаємодії та обробку запитів користувачів на визначення статусу сертифікатів з використанням протоколу визначення статусу сертифіката (OCSP) шляхом формування інформації про статус сертифікатів;

– оповіщення користувачів про зміну статусу сертифікатів засобами електронної пошти;

– приймання через сервер взаємодії та обробку запитів користувачів на формування позначок часу, шляхом формування позначок часу та передачу сформованих позначок часу користувачам;

– внесення сформованих позначок часу в базу даних;

– зберігання сформованих позначок у базі даних;

– архівування бази даних позначок часу;

– генерацію особистого та відкритого ключів ЦСК;

– уведення та використання особистого ключа ЦСК;

– створення резервних копій особистого ключа ЦСК, а також відновлення особистого ключа з резервних копій;

– формування та передачу запиту на формування сертифіката ЦСК до ЦЗО чи іншого ЦСК, якому підпорядкований цей;

– отримання та запис сертифіката ЦСК до реєстру сертифікатів;

– публікацію сертифіката ЦСК у загальнодоступних каталогах (LDAP-каталоги) та на інформаційному ресурсі ЦСК (web-сторінці);

– уведення реєстраційних даних посадових осіб до реєстру посадових осіб ЦСК;

– зберігання реєстру посадових осіб та забезпечення доступу до реєстраційних даних;

– видалення реєстраційних даних посадових осіб з реєстру;

– приймання та обробку запитів на формування сертифікатів посадових осіб ЦСК;

– формування сертифікатів посадових осіб ЦСК;

– запис сформованих сертифікатів у реєстр посадових осіб;

– використання сертифікатів посадових осіб.

Сервер взаємодії має забезпечувати:

– приймання та передачу запитів користувачів і адміністраторів реєстрації на формування сертифікатів користувачів на сервер ЦСК;

– доступ користувачів до реєстру сертифікатів у загальнодоступних каталогах (LDAP-каталогах) та на інформаційному ресурсі ЦСК (web-сторінці);

– приймання та передачу запитів користувачів та віддалених адміністраторів реєстрації на скасування, блокування чи поновлення сертифікатів користувачів на сервер ЦСК;

– доступ користувачів до списків відкликаних сертифікатів у загальнодоступних каталогах (LDAP-каталогах) та на інформаційному ресурсі ЦСК (web-сторінці);

– доступ користувачів до інформації про статус сертифікатів з використанням протоколу визначення статусу сертифіката (OCSP) шляхом приймання та передачі запитів на визначення статусу сертифіката на сервер ЦСК та передачу інформації про статус у зворотному напрямку;

– приймання та передачу запитів користувачів на формування позначок часу на сервер ЦСК;

– передачу сформованих на сервері ЦСК позначок часу користувачам;

– доступ до сертифіката ЦСК у загальнодоступних каталогах (LDAP-каталогах) та на інформаційному ресурсі ЦСК (web-сторінці).

Комутатор та інше внутрішнє комунікаційне обладнання повинне забезпечувати внутрішню взаємодію засобів комплексу та утворення ЛОМ.

РС генерації ключів користувачів повинна забезпечувати:

– генерацію особистого та відкритого ключів користувача та запис особистого ключа на носій ключової інформації (НКІ);

– формування та запис на носій інформації запиту на формування сертифіката користувача.

Міжмережевий екран повинен забезпечувати фільтрацію мережевого трафіку між зовнішніми телекомунікаційними мережами та сервером взаємодії. Детально функції міжмережевого екрану повинні бути визначені в окремому технічному завданні на КЗЗ комплексу.

РС віддаленого адміністратора реєстрації має забезпечувати:

– уведення реєстраційних даних користувачів та передачу до ЦСК;

– зміни реєстраційних даних користувачів у реєстрі ЦСК;

– видалення реєстраційних даних користувачів з реєстру ЦСК;

– приймання та введення запитів користувачів на формування сертифікатів відкритих ключів на носіях інформації;

– приймання та введення запитів користувачів на скасування, блокування чи поновлення сертифікатів на носіях інформації;

– генерації особистого та відкритого ключів адміністратора реєстрації;

– введення та використання особистих ключів віддаленого адміністратора реєстрації;

– формування та передачу запиту на формування сертифіката віддаленого адміністратора реєстрації на сервер ЦСК;

– отримання, зберігання та використання сертифіката віддаленого адміністратора реєстрації.

9.5. ВИМОГИ ДО ПРОГРАМНО-ТЕХНІЧНОГО КОМПЛЕКСУ

Вимоги до характеристик комплексу

Вимоги до програмно-технічного комплексу задаються замовником у технічному завданні. Приклад таких вимог для програмно-технічного комплексу середньої потужності наведений у таблиці 9.1 (варіант).

Таблиця 9.1. **Значення характеристик комплексу (варіант)**

Показник	Значення
Кількість користувачів, яких обслуговує комплекс	не менше 1000 000
Кількість користувачів, які можуть зареєструватися	не менше 2000 за добу
Кількість користувачів, які одночасно мають доступ до сервера взаємодії (LDAP-каталогу та web-сторінки)	не менше 5 000
Час обробки запитів користувачів на формування, блокування, поновлення та скасування сертифікатів сервером ЦСК	не більше 1 хв.
Резервне копіювання реєстру сертифікатів, реєстру користувачів, бази списків відкликаних сертифікатів і бази позначок часу	не менше 1 разу на добу

Вимоги до режимів функціонування комплексу

Комплекс повинен забезпечувати функціонування та можливість надавати доступу до ЦСК користувачам цілодобово 7 днів на тиждень. Сервер ЦСК та сервер взаємодії повинні функціонувати автоматизовано. Повинна існувати можливість встановлення двох серверів ЦСК та двох серверів взаємодії, кожний з яких виконує частину загальних функцій. Функціональні характеристики та режими експлуатації комплексу не повинні залежати від типів і характеристик технічних засобів (РС, серверів та комунікаційного обладнання).

Вимоги до експлуатації комплексу

Умови та режими експлуатації комплексу

Комплекс повинен розміщатися територіально відокремлено від ІТС і взаємодіяти з користувачами ІТС через зовнішні телекомунікаційні мережі (ЗТМ). РС віддаленого адміністратора реєстрації повинна розміщатися в складі ПТК відокремленого пункту реєстрації та взаємодіяти з комплексом через ЗТМ.

Вимоги до зберігання комплекту запасних технічних засобів

Порядок зберігання комплекту запасних технічних засобів та інсталяційних пакетів програмного забезпечення повинен бути визначений у відповідній інструкції зі складу експлуатаційної документації на комплекс або ЦСК, у складі якого він експлуатується.

Вимоги до регламенту обслуговування технічних засобів

Технічне обслуговування РС та серверів комплексу повинне виконуватися відповідно до регламенту обслуговування ПЕОМ. Технічне обслуговування комунікаційного обладнання повинне виконуватися згідно з експлуатаційною документацією або ТУ підприємства-виробника обладнання. Порядок технічного обслуговування повинен бути визначений в експлуатаційній документації на ЦСК.

Вимоги до дій у разі виникнення аварійних ситуацій

Перелік можливих аварійних ситуацій при експлуатації комплексу та вимоги до дії у разі їх виникнення повинні бути визначені у відповідній інструкції зі складу експлуатаційної документації на комплекс та ЦСК.

Вимоги до зберігання та відновлення даних

Засоби сервера ЦСК повинні підтримувати можливість автоматичного резервного копіювання реєстру сертифікатів, реєстру користувачів, бази списків відкликаних сертифікатів і бази позначок часу. Зберігання резервних копій повинне здійснюватися у приміщеннях, територіально відокремлених від приміщення, де розміщений комплекс із забезпеченням захисту від НСД. Порядок резервного копіювання та зберігання резервних копій повинен бути визначений у відповідній інструкції зі складу експлуатаційної документації на комплекс або ЦСК, у складі якого він експлуатується. Детально вимоги до зберігання та відновлення даних повинні бути визначені в окремому технічному завданні на КЗЗ комплексу.

Вимоги до персоналу, що відповідає за експлуатацію комплексу

В експлуатації комплексу повинні бути задіяні такі посадові особи:

– адміністратор безпеки;
– системний адміністратор;
– адміністратор сертифікації;
– адміністратор реєстрації;
– віддалений адміністратор реєстрації.

Загальні вимоги до посадових обов'язків зазначених осіб повинні відповідати вимогам правил посиленої сертифікації [6]. Вимоги до посадових обов'язків адміністратора безпеки повинні бути визначені в окремому технічному завданні на КЗЗ комплексу. Настанови з експлуатації засобів відповідного персоналу повинні бути визначені у відповідних інструкціях зі складу експлуатаційної документації на комплекс або ЦСК. Вимоги до підготовки персоналу та посадові обов'язки повинні бути визначені в експлуатаційній документації на ЦСК.

Вимоги до комплексу технічних засобів (варіант)

Вимоги до надійності та захисту від зовнішнього впливу

Вимоги до надійності технічних засобів, що входять до складу комплексу, повинні відповідати наступним показникам за ГОСТ 27.003-90 (група засобів II, вид – відновлюваний):

– середній наробіток на відмовлення повинний бути не менше 15 000 г;
– середній час відновлення працездатного стану не більше 0,5 г;
– середній термін служби має становити не менше 5 років;
– коефіцієнт технічного використання повинний бути не менше 0,95.

Технічні засоби комплексу повинні експлуатуватися в приміщеннях з нормальними кліматичними умовами:
– температура навколишнього середовища повітря плюс 20 ± 5 °С;
– відносна вологість (навколишнього повітря 60 ± 15) %;
– атмосферний тиск від 84 до 107 кПа (від 630 до 800 мм. рт. ст.).

Вимоги електричної та механічної безпеки повинні відповідати ГОСТ 25861-83, клас захисту від поразки електричним струмом – перший.

Технічні засоби комплексу повинні бути стійким до зовнішніх впливів і чинників відповідно до вимог, які висуваються до наземної техніки класу 1, категорії технічних засобів, призначених для експлуатації в наземних стаціонарних приміщеннях і спорудах у кліматичному виконанні ПХЛ групи 1.1 відповідно до ГОСТ 21552-84.

Вимоги до діагностування

Усі технічні засоби комплексу повинні забезпечувати можливість діагностування та отримання інформації про стан їх функціонування. При виникненні збоїв або відмов при функціонуванні засобів повинна забезпечуватися можливість сигналізації про виникнення позаштатної ситуації.

Вимоги до окремих технічних засобів (варіант)

Вимоги до складу та характеристик окремих технічних засобів (варіант), що повинні входити до складу комплексу, та вимоги й характеристики програмного забезпечення відповідних засобів наведені в табл. 9.2.

Таблиця 9.2. **Склад і характеристики окремих технічних засобів**

Технічний засіб	Тип і характеристика	Спеціальні технічні засоби	Системне програмне забезпечення	Спеціальне програмне забезпечення
1	2	3	4	5
РС адміністратора безпеки	ПЕОМ	Мають бути визначені в ЧТЗ на КЗЗ комплексу	Має бути визначене в ЧТЗ на КЗЗ комплексу	Має бути визначене в ЧТЗ на КЗЗ комплексу
РС системного адміністратора	ПЕОМ	GPS-приймач	ОС. Засоби доступу та адміністрування СУБД сервера ЦСК. Засоби доступу та адміністрування сервера взаємодії	Програмний комплекс синхронізації часу

Закінчення табл. 9.2

1	2	3	4	5
РС адміністратора реєстрації	ПЕОМ	АГВЧ	ОС. Засоби доступу до СУБД сервера ЦСК	Програмні компоненти роботи з АГВЧ. Програмний комплекс адміністратора реєстрації
РС адміністратора сертифікації	ПЕОМ	АГВЧ	ОС. Засоби доступу до СУБД сервера ЦСК	Програмні компоненти роботи з АГВЧ. Програмний комплекс адміністратора сертифікації
Сервер ЦСК	ЕОМ серверного типу	НМС. АМС. АГВЧ	ОС серверного типу. СУБД	Програмні компоненти роботи з АГВЧ та АМС. Програмний комплекс сервера ЦСК
Комутатор	Пристрій комутації ЛОМ			
Сервер взаємодії	ЕОМ серверного типу		ОС серверного типу. Модуль передачі електронних поштових повідомлень (MTA). http-сервер. LDAP-сервер	Програмний комплекс сервера взаємодії
МЕ	МЕ		Має бути визначене в ЧТЗ на КЗЗ комплексу	Має бути визначене в ЧТЗ на КЗЗ комплексу
РС генерації ключів користувачів	ПЕОМ	АГВЧ	ОС	Програмні компоненти роботи з АГВЧ. Програмний комплекс генерації ключів користувачів
РС віддаленого адміністратора реєстрації	ПЕОМ	АГВЧ	ОС	Програмні компоненти роботи з АГВЧ. Програмний комплекс віддаленого адміністратора реєстрації

До складу всіх технічних засобів повинні входити джерела безперебійного живлення.

До складу засобів РС адміністратора сертифікації, адміністратора реєстрації, віддаленого адміністратора реєстрації, генерації ключів користувачів і сервера ЦСК повинен входити апаратний генератор випадкових чисел (АГВЧ), призначений для генерації послідовностей випадкових чисел під час генерації ключових даних програмними комплексами.

До складу сервера ЦСК повинен входити апаратний модуль сертифікації (АМС), призначений для:

– управління особистим ключем ЦСК (генерації, зберігання, введення, використання, резервного копіювання, відновлення та знищення);

– формування ЕЦП з використанням особистого ключа ЦСК.

Окремі зразки апаратних генераторів випадкових чисел та апаратних модулів сертифікації повинні отримати експертний висновок у галузі КЗІ ДСТСЗІ СБ України у складі комплексу.

До складу сервера ЦСК повинен входити пристрій резервного копіювання – накопичувач на магнітній стрічці (НМС), призначений для запису на касети резервних копій даних і створення довгострокових архівів даних з сервера ЦСК.

До складу РС системного адміністратора повинен входити GPS-приймач, призначений для отримання сигналів точного часу від GPS-супутників. Точність синхронізації часу не повинна перевищувати 1 с. Методика синхронізації часу з GPS-супутниками та синхронізації часу між технічними засобами комплексу в ЛОМ повинна бути погоджена з ДСТСЗІ СБ України у встановленому порядку.

Вимоги до розміщення та взаємодії технічних засобів

Структурна схема комплексу технічних засобів наведена на рис. 9.3.

РС адміністратора безпеки, системного адміністратора, адміністратора реєстрації, адміністратора сертифікації, сервер ЦСК та сервер взаємодії повинні взаємодіяти через внутрішню телекомунікаційну мережу на основі кабельної мережі та комутатора й утворювати ЛОМ.

Сервер ЦСК, його ДБЖ, НМС, монітор і пристрої введення повинні бути розміщені у стійці в спеціальному приміщенні та підключатися до комутатора через волоконно-оптичну лінію зв'язку (ВОЛЗ).

Сервер взаємодії, його ДБЖ, монітор та пристрої введення, а також комутатор та міжмережевий екран повинні бути розміщені в окремій шафі.

Сервер взаємодії повинен підключатися до зовнішньої телекомунікаційної мережі через міжмережевий екран. Для підключення до комутатора та до МЕ повинні використовуватися різні мережеві адаптери.

Міжмережевий екран повинен підключатися до зовнішньої телекомунікаційної мережі через комунікаційне обладнання оператора послуг передачі даних.

Комплекс повинен взаємодіяти з ПТК інших ЦСК (у тому числі й ЦЗО), ІТС користувачів та РС віддалених адміністраторів реєстрації (ПТК відокремлених пунктів реєстрації) через сервер взаємодії.

Інші вимоги щодо розміщення та взаємодії технічних засобів з урахуванням вимог захисту оброблюваної інформації від НСД повинні бути визначені у ЧТЗ на КЗЗ комплексу.

Основним елементом інфраструктури системи ЕЦП (відкритих ключів) України є центр сертифікації ключів. Система ЕЦП (інфраструктура відкритих ключів) за своєю суттю являє собою сукупність взаємодіючих між собою центрів сертифікації ключів.

9.5. АКРЕДИТОВАНИЙ ЦЕНТР СЕРТИФІКАЦІЇ КЛЮЧІВ

Акредитований центр сертифікації ключів (АЦСК) – основний уповноважений орган системи ЕЦП (інфраструктури відкритих ключів), основними функціями якого є реєстрація користувачів (далі – Абонентів), формування їм сертифікатів відкритих ключів та управління життєвим циклом сертифікатів.

9.5.1. Технічна структура програмно-технічного комплексу

Програмно-технічний комплекс (ПТК) Центру є технічною основою автоматизованої системи Центру та забезпечує технологічну реалізацію таких регламентних процедур Центру з обслуговування сертифікатів Абонентів:

– реєстрацію Абонентів, які обслуговуються Центром;

– ведення реєстру Абонентів;

– додавання, зміну та видалення реєстраційних даних Абонентів з реєстру Абонентів;

– архівування та резервне копіювання реєстру Абонентів;

– приймання та реєстрацію запитів Абонентів на формування сертифікатів;

– формування сертифікатів;

– внесення сформованих сертифікатів у реєстр сертифікатів;

– архівування та резервне копіювання реєстру сертифікатів;

– приймання та реєстрацію запитів Абонентів на скасування, блокування чи поновлення сертифікатів;

– скасування, блокування або поновлення сертифікатів на основі запитів;

– зберігання запитів, отриманих від Абонентів, у базі даних запитів;

– архівування й резервне копіювання бази даних запитів;

– внесення інформації про поточний статус сертифіката до реєстру сертифікатів;

– формування списків відкликаних сертифікатів користувачів;

– публікацію списків відкликаних сертифікатів у загальнодоступних каталогах (LDAP-каталоги) та на інформаційному ресурсі Центру (web-сторінці);

– надання доступу користувачів до списків відкликаних сертифікатів у загальнодоступних каталогах (LDAP-каталогах) та на інформаційному ресурсі Центру (web-сторінці);

– інформування Абонентів про зміну статусу сертифікатів засобами електронної пошти;

– надання послуг фіксування часу;

– забезпечення захисту інформації, що обробляється та захисту технічних засобів від НСД.

До складу програмно-технічного комплексу входять такі технічні засоби:

– сервери ЦСК;

– сервери взаємодії;

– робоча станція (РС) адміністратора реєстрації;
– РС адміністратора сертифікації;
– РС адміністратора безпеки;
– РС системного адміністратора;
– комутатор, міжмережевий екран та інше комунікаційне обладнання;
– РС генерації ключів користувачів;
– РС віддалених адміністраторів реєстрації зі складу ПТК відокремлених пунктів реєстрації.

Функціональна схема ПТК Центру наведена на рис. 9.4.

Структурна схема комплексу технічних засобів ПТК Центру наведена на рис. 9.5.

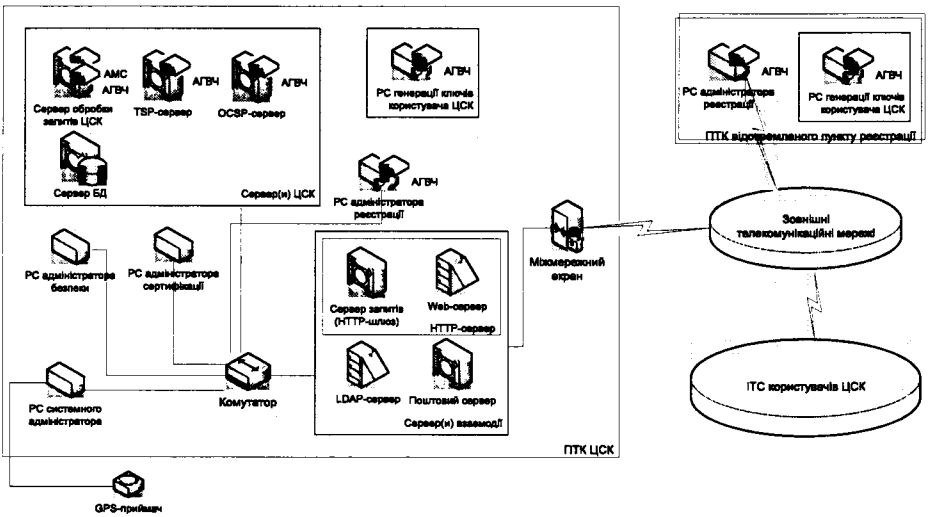

Рис. 9.4. Функціональна схема ПТК Центру

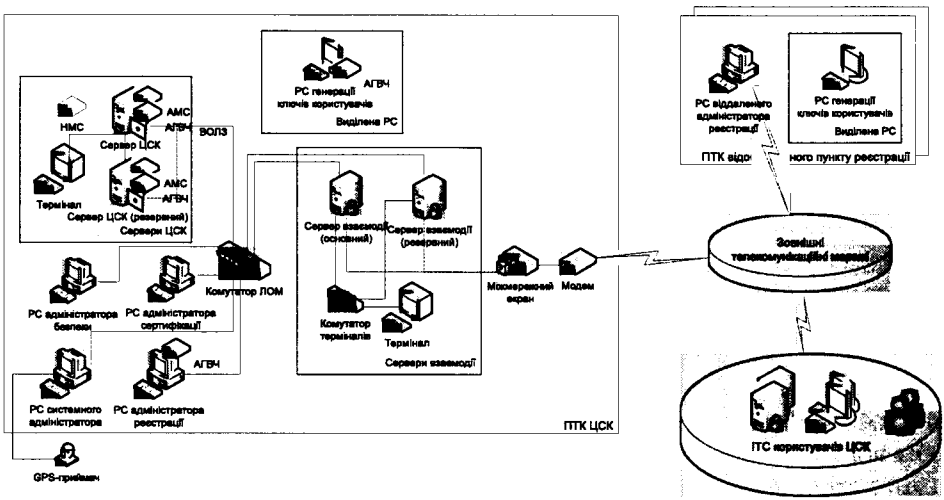

Рис. 9.5. Структурна схема комплексу технічних засобів ПТК Центру

РС адміністратора безпеки, системного адміністратора, адміністратора реєстрації, адміністратора сертифікації, сервер ЦСК та сервер взаємодії взаємодіють через внутрішню телекомунікаційну мережу на основі кабельної мережі та комутатора й утворюють ЛОМ.

Сервер ЦСК, його джерело безперервного живлення, накопичувач на магнітній стрічці, монітор і пристрої введення розміщені в стійці у спеціальному приміщенні та підключені до комутатора через волоконно-оптичну лінію зв'язку.

Сервер взаємодії, його джерело безперервного живлення, монітор та пристрої введення, а також комутатор та міжмережевий екран розміщені в окремій шафі.

Сервер взаємодії підключено до зовнішньої телекомунікаційної мережі через міжмережевий екран. Підключення до комутатора та до міжмережевого екрана здійснюється за допомогою різних мережевих адаптерів.

Міжмережевий екран підключено до зовнішньої телекомунікаційної мережі через комунікаційне обладнання оператора послуг передачі даних.

Комплекс взаємодіє з ПТК інших центрів (у тому числі й Центральним засвідчувальним органом), інформаційно-телекомунікаційних систем Абонентів (користувачів) та РС віддалених адміністраторів реєстрації (ПТК Відокремлених пунктів реєстрації) через сервер взаємодії.

Схеми взаємодії технічних засобів Абонентів (користувачів ЦСК) з ПТК Центру наведені на рис. 9.4, 9.5.

9.5.2. Режими функціонування та експлуатації програмно-технічного комплексу

Комплекс дозволяє функціонувати та надає можливість доступу до АЦСК Абонентам цілодобово або за іншими умовами, визначеними Регламентом АЦСК.

Обробка запитів Абонентів виконується автоматизовано з можливістю управління процесом обробки в ручному режимі або тільки в ручному режимі.

Усі технічні засоби комплексу забезпечують можливість діагностування та отримання інформації про стан їх функціонування.

При виникненні збоїв або відмов при функціонуванні засобів забезпечується сигналізація про виникнення позаштатної ситуації.

Комплекс забезпечує такі характеристики:

– кількість Абонентів, яких обслуговує комплекс, складає не менше 1 000 000;

– кількість Абонентів, які можуть зареєструватися, складає не менше 1 000 за добу;

– кількість Абонентів, запити яких одночасно обробляються комплексом, складає 1 в ручному режимі та не менше 10 в автоматизованому;

– час обробки запитів Абонентів складає не більше 2 годин в ручному режимі та не більше 5 хвилин в автоматизованому;

– резервне копіювання електронного реєстру сертифікатів Абонентів, запитів на сертифікацію та списків відкликаних сертифікатів складає не менше 1 разу на добу.

Комплекс розміщується у виділених приміщеннях і взаємодіє з Абонентами через телекомунікаційні канали.

9.5.3. Склад і функціональні обов'язки персоналу, що відповідає за експлуатацію програмно-технічного комплексу

Персонал, що відповідає за експлуатацію програмно-технічного комплексу, включає:

– адміністратора сертифікації;

– адміністратора реєстрації;

– адміністратора безпеки;

– системного адміністратора.

До складу елементів АЦСК входять такі робочі пости:

– пост «Автоматизоване робоче місце (АРМ) Адміністратора сертифікації», призначений для забезпечення управління процесом обробки запитів центрів;

– пост «АРМ Адміністратора реєстрації», призначений для ведення реєстрів центрів;

– пост «АРМ Адміністратора безпеки», призначений для адміністрування КЗЗ КСЗІ комплексу;

– пост «АРМ Системного адміністратора», призначений для адміністрування програмно-технічних засобів комплексу.

9.5.4. Управління АЦСК

Для управління АЦСК створюється система управління центру, що охоплює:

– органи управління;

– пункт управління елементами АЦСК;

– мережі службового зв'язку та автоматичного контролю стану комунікаційного обладнання, КЗЗ інформації.

До складу органів управління АЦСК входять начальник АЦСК та черговий АЦСК. До складу органів управління елемента АЦСК входять начальник і черговий елемента АЦСК.

Пункт управління АЦСК – спеціально обладнане та оснащене технічними засобами місце, з якого начальник АЦСК (елемента АЦСК) особисто або через чергового АЦСК здійснює керівництво підлеглими підрозділами (черговою зміною).

Пункт управління АЦСК розташовується в спеціальних приміщеннях (апаратних), у яких обладнано робочі місця для чергової обслуги (начальника АЦСК) і чергового АЦСК.

Пункти управління елементами АЦСК обладнуються в одній із апаратних, де є робоче місце для начальника центру (чергового центру).

Управління встановленням інформаційного обміну АЦСК штатні посадові особи виконують особисто та через чергового АЦСК (елемента АЦСК).

Для забезпечення управління АЦСК використовується внутрішня вузлова мережа гучномовців і телефонного службового зв'язку, автоматичного телефонного зв'язку.

Службовий гучномовний і телефонний зв'язок на АЦСК забезпечується по виділених парах з'єднувальних ліній.

Органи управління контролюють хід виконання особовим складом чергових змін АЦСК завдань з обробки інформації безпосередньо на елементах АЦСК, а також на підставі доповідей підлеглих і за даними системи автоматизованого контролю про стан обміну інформацією. Результати контролю реєструються пристроями автоматичної реєстрації та відображуються в оперативно-технічній документації.

Під терміном ***обробка інформації*** в подальшому розумітимемо виконання однієї чи декількох операцій, зокрема збирання, введення, записування, перетворення, зчитування, зберігання, знищення, реєстрацію, приймання, отримання, передавання, які здійснюються в АЦСК при виконанні ним своїх функцій за допомогою технічних і програмних засобів.

Взаємодія між елементами АЦСК організовується та підтримується за умови оперативного й ефективного використання телекомунікаційного обладнання, функціонально взаємопов'язаних систем зв'язку, узгоджених дій посадових осіб чергової зміни при виконанні поставлених завдань.

Межі відповідальності між елементами АЦСК встановлює начальник АЦСК, а між робочими постами – начальник елемента АЦСК, що відображується у затверджених інструкціях, схемах тощо.

Взаємовідносини посадових осіб та осіб чергової зміни елементів АЦСК регламентуються функціональними обов'язками та відповідними документами з оперативно-технічної служби.

9.5.5. Регламент АЦСК

Регламент АЦСК [29, 30] є нормативним документом, що визначає організаційні, технічні та інші умови діяльності центру сертифікації ключів відомства під час надання послуг електронного цифрового підпису, встановлює порядок роботи центру сертифікації ключів з надання послуг електронного цифрового підпису (далі – ЕЦП).

Норми Регламенту поширюються на:

– центр сертифікації ключів (далі – Центр);

– відокремлені пункти реєстрації заявників (далі – Відокремлені пункти реєстрації);

– користувачів послуг – Абонентів: юридичних осіб публічного та приватного права всіх форм власності, фізичних осіб – суб'єктів підприємницької діяльності, фізичних осіб – громадян України, осіб без громадянства, іноземців.

Чітке дотримання та виконання умов Регламенту для вищенаведених осіб є обов'язковим.

Будь-яка зацікавлена особа може ознайомитися з положеннями Регламенту на електронному інформаційному ресурсі, в офісах Центру та його відокремлених пунктів.

Регламент розроблюється у відповідності до:

– Закону України «Про електронний цифровий підпис»;

– Порядку засвідчення наявності електронного документа (електронних даних) на певний момент часу, затвердженому постановою Кабінету Міністрів України від 26 травня 2004 року № 680;

– Порядку акредитації центру сертифікації ключів, затвердженому постановою Кабінету Міністрів України від 13 липня 2004 року № 903;

– Наказу ДСТСЗІ СБ України від 10.05.2006 № 50 «Про внесення змін до Правил посиленої сертифікації».

Терміни та визначення, що вживаються в Регламенті, визначені вищенаведеними нормативними актами.

Центр здійснює свою діяльність у сфері електронного документообігу, застосування ЕЦП органами державної влади, органами місцевого самоврядування, підприємствами, установами й організаціями всіх форм власності, іншими суб'єктами господарської діяльності та фізичними особами.

Діяльність Центру не поширюється на відносини, що виникають під час використання інших видів електронного підпису, у тому числі переведеного в цифрову форму зображення власноручного підпису.

Центр надає послуги ЕЦП та здійснює діяльність на підставі Регламенту, який погоджується з контролюючим органом.

Під послугами ЕЦП розуміють надання у користування засобів електронного цифрового підпису, допомогу при генерації відкритих та особистих ключів, обслуговування сертифікатів ключів (формування, розповсюдження, скасування, зберігання, блокування та поновлення), надання інформації щодо чинних, скасованих і блокованих сертифікатів ключів, послуги фіксування часу, консультації та інші послуги, визначені Законом України від 22.05.2003 № 852-IV «Про електронний цифровий підпис».

Основною послугою Центру є обслуговування сертифікатів відкритих ключів (далі – сертифікатів) Абонентів, що включає:

– реєстрацію Абонентів;

– надання Абонентам засобів ЕЦП та шифрування даних, засобів генерації особистих і відкритих ключів;

– сертифікацію відкритих ключів Абонентів;

– розповсюдження сертифікатів;

– управління статусом сертифікатів та розповсюдження інформації про статус сертифікатів;

– надання послуг фіксування часу.

Окрім надання послуг ЕЦП, Центр надає консультаційні послуги за зверненням Абонентів.

Надання вищезазначених послуг здійснюється Центром на підставі укладених договорів безпосередньо або через відокремлені пункти реєстрації заявників.

Ці пункти є відособленими підрозділами без правового статусу юридичної особи, що реалізують функції Центру з реєстрації Абонентів та їх подальшого обслуговування на відповідній території.

Відокремлені пункти діють на підставі Положення про відокремлений пункт і Регламенту.

Безпосереднє управління відокремленими пунктами здійснюється Центром сертифікації ключів.

9.5.6. Умови, процедури, механізми надання послуг абонентам

Порядок реєстрації та ідентифікації абонентів

Під реєстрацією Абонента розуміють внесення інформації про Абонента до реєстру Абонентів Центру.

Абонент може бути представлений довірчою особою, якщо немає можливості його особистої присутності в Центрі. У цьому випадку Абонент надає доручення на подання документів для реєстрації.

Доручення засвідчується:

– для юридичних осіб: підписом керівника з прикладенням печатки організації;

– для фізичних осіб: нотаріально.

Для реєстрації Абонент або його довірча особа надають до Центру такі документи:

Для юридичних осіб:

– заява на реєстрацію;

– нотаріально засвідчена копія свідоцтва про державну реєстрацію суб'єкта підприємництв;

– документи, що підтверджують повноваження керівника заявника;

– копія свідоцтва про реєстрацію платника ПДВ (у разі якщо особа є платником податку на додану вартість);

– доручення.

Для фізичних осіб:

– заява на реєстрацію;

– копії 1–4, 11–12 сторінок паспорту, засвідчені підписом особи;

– копію ідентифікаційного коду;

– доручення.

Адміністратор реєстрації Центру або віддалений адміністратор реєстрації (Відокремлений пункт реєстрації) виконує процедуру ідентифікації Абонента (його довірчої особи), що проходить процедуру реєстрації, шляхом установлення особи за паспортом або іншим документом, що засвідчує особу.

Після позитивної ідентифікації Абонента (його довірчої особи) адміністратор реєстрації Центру або віддалений адміністратор реєстрації приймає та розглядає документи, надані Абонентом (його довірчою особою).

Заява на реєстрацію розглядається адміністратором реєстрації Центру або віддаленим адміністратором реєстрації протягом однієї години з моменту надходження заяви.

У випадку відмови в реєстрації заява на реєстрацію разом з додатками повертається заявнику з позначкою адміністратора реєстрації Центру або віддаленого адміністратора реєстрації.

Якщо прийнято позитивне рішення, адміністратор реєстрації Центру або віддалений адміністратор реєстрації здійснює підготовку договору про надання послуг ЕЦП, який підписує Абонент (його довірча особа) і посадова особа Центру, що має на це повноваження.

Після підписання договору та оплати Абонентом послуг ЕЦП адміністратор реєстрації Центру або віддалений адміністратор реєстрації виконує реєстраційні дії щодо занесення реєстраційної інформації до реєстру Абонентів Центру.

Порядок генерації ключів Абонента

Відкритий та особистий ключі Абонента можуть бути генеровані:

– на робочому місці Абонента;

– на робочій станції генерації ключів Абонентів у Центрі.

Для генерації відкритого й особистого ключів на робочому місці Абонента застосовуються засоби, що надаються Центром. При цьому генерація здійснюється з використанням технічних засобів Абонента. Генерований особистий ключ Абонента захищається паролем та записується на носій ключової інформації. Відповідальність за забезпечення конфіденційності та цілісності особистого ключа несе Абонент.

Засоби генерації ключів формують запит на формування сертифіката у відповідному форматі, що містить відкритий ключ Абонента та додаткову інформацію для формування сертифіката в Центрі.

Передача до Центру сформованого Абонентом запиту здійснюється на носії інформації особисто Абонентом або його довірчою особою після реєстрації Абонента.

У разі генерації відкритого й особистого ключа Абонента в Центрі ключі генеруються ним особисто на робочій станції генерації ключів Абонентів, що входить до складу програмно-технічного комплексу Центру. Особистий ключ Абонента записується на носій ключової інформації та залишається в Абонента, а сформований запит на формування сертифіката передається через службовий носій інформації на робочу станцію адміністратора реєстрації.

Під час обробки запиту на формування сертифіката Абонента здійснюється перевірка володіння Абонентом особистого ключа, відповідний якому відкритий ключ міститься в запиті. Перевірка здійснюється шляхом перевірки ЕЦП, накладеного на запит на формування сертифіката, з використанням відкритого ключа, що міститься в запиті. Тобто запит на формування сертифіката є самопідписаним.

Особисті ключі Абонентів не зберігаються в Центрі. Після генерації та запису на носій ключової інформації вони знищуються надійним способом.

Строк дії особистого ключа Абонента не повинен перевищувати 2 роки. Початком строку дії особистого ключа Абонента вважається дата й час формування сертифіката, що містить відкритий ключ, відповідний до особистого.

Порядок формування сертифікатів та надання їх Абонентам

Для формування сертифіката Абонентом або його довірчою особою в Центр повинні бути передані документи відповідно до вищезазначеного переліку, електронний запит на формування сертифіката у відповідному форматі.

Адміністратор реєстрації Центру або віддалений адміністратор реєстрації виконує процедуру ідентифікації Абонента.

При ухваленні позитивного рішення адміністратор реєстрації надсилає електронний запит на формування сертифіката на сервер обробки запитів Центру.

Після формування сертифіката адміністратор реєстрації виготовляє три копії сертифіката у вигляді документа в паперовій формі. Усі копії сертифікатів засвідчуються печаткою Центру, власноручним підписом Абонента або підписом його довірчої особи, а також власноручним підписом адміністратора реєстрації.

У разі реєстрації Абонента через відокремлений пункт реєстрації заявників копії сертифіката в паперовій формі виготовляє, завіряє печаткою та підписує віддалений адміністратор реєстрації.

Сертифікат в електронній формі записується на носій інформації Абонента та в реєстр сертифікатів Центра.

Строк чинності сертифіката Абонента зазначається в сертифікаті та не перевищує 2 роки. Початком строку чинності сертифіката Абонента вважається дата й час його формування.

Порядок блокування, поновлення та скасування сертифікатів

Абонент зобов'язаний виконати дії зі скасування сертифіката в разі:

– компрометації особистого ключа Абонента;

– зміни відомостей, зазначених у сертифікаті;

– зміни обставин, на підставі яких було надано право підпису.

Компрометація ключа Абонента – це:

– факт або обґрунтована підозра того, що особистий ключ Абонента став відомий іншим особам;

– факт втрати Абонентом можливості подальшого використання особистого ключа через будь-які обставини (зокрема фізичне пошкодження або втрата носія, неможливість відтворити пароль захисту).

У разі компрометації ключа Абонент зобов'язаний терміново сповістити про цей факт Центр і виконати дії щодо блокування сертифікатів.

Зміна будь-якого з реквізитів, зазначених у сертифікаті, потребує його скасування.

Зокрема, до таких причин належать:

– переведення на іншу посаду або звільнення з роботи власника сертифіката (для сертифікатів ключів юридичних осіб/ посадових осіб);

– зміна прізвища;

– зміна місця прописки/ реєстрації в частині, що вказана в реквізитах власника сертифіката;

– виявлення помилок у реквізитах тощо;

– зміна зовнішніх обставин, які навіть при збереженні реквізитів власника сертифіката змінюють його статус, що впливає на правомочність підпису, зокрема зміна положення про посаду власника ключа, що призводить до того, що зазначені в сертифікаті повноваження більше не належать власнику ключа (у тому числі втрата права підпису звітності, керування банківським рахунком тощо).

У разі виникнення будь-яких причин та обставин, зазначених вище, Абонент зобов'язаний невідкладно заблокувати сертифікат та протягом терміну дії блокування виконати операції зі скасування сертифіката.

Дозволяється виконувати безпосередньо скасування сертифіката (обминаючи фазу його блокування), якщо Абонент вважає, що виконання операції відкликання в такий спосіб суттєво не вплине на термін чинності сертифіката, що відкликається.

Блокування тимчасово припиняє дію сертифіката. Після блокування сертифіката Абонент зобов'язаний або поновити сертифікат, або виконати дії щодо

скасування сертифіката у відповідності з Регламентом Центру. У разі якщо Абонент не виконає поновлення сертифіката протягом 1 календарного місяця, сертифікат автоматично скасовується Центром.

Для здійснення блокування сертифіката Абонент подає заяву на блокування до Центру.

Блокування сертифіката здійснюється Центром на підставі заяви, що надходить установленим порядком до Центру в усній або паперовій формі, чи у вигляді електронного запиту.

Часом блокування сертифіката вважається час офіційного повідомлення Абонента про блокування.

Усна заява та заява у вигляді електронного запиту повинна бути підтверджена письмовою заявою Абонента протягом 7 (семи) робочих днів з часу прийняття Центром усної заяви Абонента або електронного запиту на блокування.

Заява в усній формі подається в Центр за телефоном.

Заявник повинен повідомити адміністратору реєстрації Центру або віддаленому адміністратору реєстрації таку інформацію:

– реєстраційний номер Заявника;
– ідентифікаційні дані власника сертифіката;
– ключову фразу парольної автентифікації;
– реєстраційний номер сертифіката.

Заява в усній формі приймається тільки у разі позитивної автентифікації (збігу парольної фрази переданої в заяві з інформацією з реєстру Абонентів).

Подача й обробка усної заяви здійснюється цілодобово. Обробка усної заяви на блокування сертифіката та інформування Абонента здійснюється протягом тридцяти хвилин з моменту подачі заяви.

Заява в паперовій формі подається в Центр за відповідною формою.

Заява на блокування сертифіката засвідчується власноручним підписом власника сертифіката.

Подача заяви на блокування сертифіката в Центр та її розгляд здійснюється тільки протягом робочого дня.

Обробка заяви в паперовій формі на блокування сертифіката та інформування Абонента про блокування повинні бути здійснені протягом одного робочого дня, що йде за робочим днем, протягом якого була подана заява в Центр.

Електронний запит на блокування сертифіката передається в програмно-технічний комплекс Центру у вигляді вкладення електронного поштового листа чи у вигляді http-запиту.

Електронний запит формується Абонентом програмними засобами, які надаються Центром.

Електронний запит на блокування сертифіката засвідчується власним ЕЦП власника сертифіката.

У разі передачі запиту на блокування сертифіката у вигляді http-запиту, обробка запиту та інформування Абонента про блокування здійснюються в режимі реального часу.

У разі передачі запиту на блокування сертифіката засобами електронної пошти обробка запиту та інформування Абонента про блокування повинні бути здійснені протягом 2 (двох) годин після отримання запиту Центром.

Для скасування сертифіката Абонент подає заяву на скасування до Центру.

Скасування сертифіката здійснюється Центром на підставі заяви, що надходить установленим порядком до Центру в паперовій формі.

Заява на скасування сертифіката подається в Центр за відповідною формою та засвідчується підписом власника сертифіката.

Подача заяви на скасування сертифіката в Центр та її розгляд здійснюється тільки протягом робочого дня.

Обробка заяви на скасування сертифіката та інформування Абонента про скасування повинні бути здійснені протягом одного робочого дня, що йде за робочим днем, протягом якого була подана заява до Центру.

Часом скасування сертифіката вважається час офіційного повідомлення Абонента про скасування.

Скасування припиняє дію сертифіката. Скасовані сертифікати поновленню не підлягають.

У разі припинення діяльності організації (для ключів юридичних осіб/ посадових осіб) організація, реквізити якої зазначені в сертифікаті (сертифікатах), звертається до Центру й подає:

– письмову заву встановленого зразка про скасування всіх сертифікатів організації, яку засвідчено підписом керівника та печаткою;

– довідку встановленого зразка про припинення діяльності, надану відповідним державним органом.

При скасуванні сертифікатів у зазначеному випадку скасовуються всі чинні на момент скасування сертифікати, у яких код ЄДРПОУ організації співпадає з кодом ЄДРПОУ організації, що припинила діяльність.

Поновлення чинності сертифіката ключа можливе лише для сертифікатів, які заблоковані і термін блокування не минув. Скасовані сертифікати поновленню не підлягають.

Поновлення чинності сертифіката здійснюється Центром на підставі заяви, що надходить установленим порядком до Центру в паперовій формі.

Заява в паперовій формі подається в Центр за відповідною формою.

Заява на поновлення чинності сертифіката засвідчується власноручним підписом власника сертифіката.

Подача заяви на поновлення чинності сертифіката в Центр та її розгляд здійснюється тільки протягом робочого дня.

Обробка заяви в паперовій формі на поновлення чинності сертифіката та інформування Абонента про поновлення повинні бути здійснені протягом одного робочого дня, що йде за робочим днем, протягом якого була подана заява в Центр.

Часом поновлення чинності сертифіката вважається час офіційного повідомлення Абонента про поновлення.

Порядок розповсюдження (публікації) інформації Центром про інформаційний ресурс Центру

Інформаційний ресурс Центру призначений для розміщення на ньому відкритої інформації, яка структурно поділяється на:

– довідкову інформацію (режими роботи Центру, положення Регламенту, нормативні документи, договори на надання послуг, форми заяв тощо);

– сертифікат Центру;

– сертифікати серверів Центру;

– сертифікати Абонентів;

– списки відкликаних сертифікатів, що містять інформацію про статуси сертифікатів Центру та Абонентів.

Електронна адреса (DNS-ім'я) електронного інформаційного ресурсу є публічною.

Технічною основою інформаційного ресурсу Центру є сервери взаємодії, що входять до складу програмно-технічного комплексу Центру.

Довідкова інформація розміщується на http-сервері сервера взаємодії у вигляді набору web-сторінок.

Сертифікат Центру, сертифікати серверів Центру та Абонентів, а також списки відкликаних сертифікатів розміщуються:

– у складі web-сторінок на http-сервері сервера взаємодії;

– в інформаційному дереві LDAP-каталогу на LDAP-сервері сервера взаємодії.

Доступ до http-сервера здійснюється за DNS-ім'ям за протоколом http (номер TCP-порту 80).

Доступ до LDAP-сервера здійснюється за DNS-ім'ям за протоколом LDAP (номер TCP-порту 389).

Порядок публікації сертифіката Центру та сертифікатів серверів Центру

Після формування сертифіката Центра виконується його публікація на інформаційний ресурс. Окрім власного сертифіката Центру, виконується публікація сертифікатів серверів Центру:

– сервера обробки запитів (CMP-сервера);

– сервера позначок часу (TSP-сервера);

– сервера визначення статусу сертифікатів (OCSP-сервера).

Публікація сертифікатів серверів Центру виконується після формування сертифіката відповідного сервера.

Порядок публікації сертифікатів Абонентів

Публікація сертифікатів Абонентів на інформаційний ресурс Центру здійснюється за згодою Абонента. Інформація про необхідність публікації сертифікатів кожного окремого Абонента вноситься до складу реєстраційних даних під час реєстрації Абонента.

Публікація сертифікатів Абонентів в інформаційному дереві LDAP-каталога здійснюється автоматично з інтервалом синхронізації 15 хв.

Порядок публікації списків відкликаних сертифікатів

Публікація списків відкликаних сертифікатів Абонентів на інформаційний ресурс Центру (на http-сервері) здійснюється відразу ж після його випуску.

Центр виконує випуск списків відкликаних сертифікатів двох типів:

– повний список;

– частковий список.

Повний список випускається один раз на тиждень і місить інформацію про всі відкликані сертифікати, які були сформовані Центром на діючому особистому ключі.

Частковий список випускається кожні дві години та місить інформацію про всі відкликані сертифікати, статус яких був змінений в інтервалі між часом випуску останнього повного списку та часом формування поточного часткового списку.

Публікація списків відкликаних сертифікатів в інформаційному дереві LDAP-каталогу здійснюється автоматично з інтервалом синхронізації 5 хв.

9.6. КОМПЛЕКСНА СИСТЕМА ЗАХИСТУ ІНФОРМАЦІЇ ЦЕНТРУ

9.6.1. Призначення комплексної системи захисту інформації Центру

Комплексна система захисту інформації в автоматизованій системі Центру призначена для [229]:

– реалізації політики безпеки інформації Центру;

– забезпечення конфіденційності, цілісності, доступності інформації під час експлуатації автоматизованої системи Центру;

– недопущення витоку інформації з обмеженим доступом і втрати її матеріальних носіїв;

– створення механізму та умов оперативного реагування на зовнішні та внутрішні загрози з метою забезпечення безпеки інформації й оперативного оповіщення адміністраторів безпеки про факти несанкціонованого доступу до інформації;

– ефективного попередження, своєчасного виявлення та знешкодження загроз для ресурсів обчислювальної системи Центру, причин та умов, які спричиняють або можуть призвести до порушення її нормального функціонування;

– керування засобами захисту інформації, розмежування доступу користувачів до ресурсів автоматизованої системи Центру, контроль за їхньою роботою з боку осіб, які відповідають за забезпечення безпеки інформації в Центрі;

– створення умов для забезпечення максимально можливого рівня локалізації негативних наслідків, що завдаються неправомірними та несанкціонованими діями порушників; зменшення негативного впливу наслідків порушення безпеки на функціонування Центру;

– організації обліку, зберігання, обігу інформації, яка потребує захисту, і матеріальних носіїв, на яких вона накопичується;

– реєстрації, збору, зберігання, обробки даних про всі події в Центрі, які мають відношення до безпеки інформації;

– забезпечення доступності ресурсів автоматизованої системи Центру для її користувачів.

Схема взаємодії технічних засобів Абонентів (користувачів ЦСК) з ПТК Центру подана на рис. 9.6.

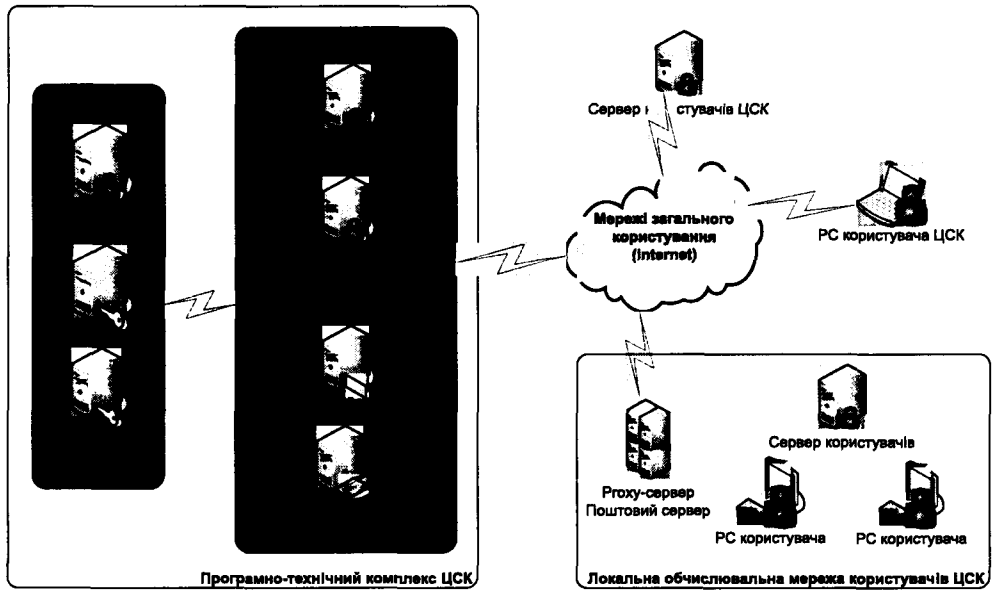

Рис. 9.6. Схема взаємодії технічних засобів Абонентів (користувачів ЦСК) з ПТК Центру

9.6.2. Організаційна структура Центру

До складу Центру входять:

– підрозділ реєстрації та обслуговування Абонентів;

– підрозділ сертифікації ключів;

– служба захисту інформації;

– підрозділ технічного обслуговування програмно-технічного комплексу Центру;

– відокремлені пункти реєстрації.

До складу Центру можуть входити й інші підрозділи, що забезпечують його роботу.

Підрозділ реєстрації та обслуговування Абонентів

До складу підрозділу реєстрації та обслуговування Абонентів входять:

– оператори реєстрації (діловоди);

– адміністратори реєстрації (головний та чергова зміна).

Функції та завдання підрозділу реєстрації та обслуговування Абонентів:

– встановлення осіб, які звернулися до Центру з метою формування сертифіката;

– перевірка даних, обов'язкових для формування сертифіката, а також даних, які вносяться в сертифікат на вимогу Абонента;

– підготовка договору про надання послуг ЕЦП;

– отримання від Абонентів заявок на формування, скасування, блокування та поновлення сертифікатів ключів;

– надання допомоги Абонентам під час генерації особистих і відкритих ключів у разі отримання від них відповідного звернення та вжиття заходів щодо забезпечення безпеки інформації під час генерації;

– перевірка законності звернень про блокування, поновлення та скасування сертифікатів;

– надання Абонентам консультацій щодо умов та порядку надання послуг ЕЦП.

Підрозділ сертифікації ключів

До складу підрозділу сертифікації ключів входить адміністратор сертифікації.

Функції та завдання підрозділу сертифікації ключів:

– формування за допомогою особистого ключа Центру сертифікатів Абонентів, списків відкликаних сертифікатів і позначок часу;

– публікація сертифікатів і списків відкликаних сертифікатів;

– ведення, архівація та відновлення реєстру сформованих сертифікатів;

– подання до Центрального засвідчувального органу даних, необхідних для формування сертифіката та засвідчення відкритого ключа Центру;

– контроль за веденням журналів прийому-передачі ключів.

Служба захисту інформації

До складу служби захисту інформації входять:

– керівник служби захисту інформації;

– адміністратор безпеки.

Функції та завдання служби захисту інформації:

– забезпечення повноти та якісного виконання організаційно-технічних заходів із захисту інформації;

– розроблення розпорядчих документів, згідно з якими в Центрі повинен забезпечуватися захист інформації, контроль за їх виконанням;

– своєчасне реагування на спроби несанкціонованого доступу до ресурсів програмно-технічного комплексу Центру, порушення правил експлуатації засобів захисту інформації;

– контроль за зберіганням особистого ключа Центру та його резервної копії, особистих ключів посадових осіб Центру;

– участь у знищенні особистого ключа Центру, контроль за правильним і своєчасним знищенням посадовими особами особистих ключів;

– ведення контролю за процесом резервування сертифікатів ключів і списків відкликаних сертифікатів, а також інших важливих ресурсів;

– організація розмежування доступу до ресурсів програмно-технічного комплексу Центру, зокрема розподілення між посадовими особами паролів, ключів, сертифікатів тощо;

– забезпечення спостереження (реєстрація та аудит подій в програмно-технічному комплексі Центру, моніторинг подій тощо) за функціонуванням комплексної системи захисту інформації;

– забезпечення організації та проведення заходів з модернізації, тестування, оперативного відновлення функціонування комплексної системи захисту інформації після збоїв, відмов, аварій програмно-технічного комплексу;

– ведення журналу обліку адміністратора безпеки.

Підрозділ технічного обслуговування програмно-технічного комплексу Центру

До складу підрозділу технічного обслуговування програмно-технічного комплексу Центру входять системні адміністратори (головний і чергова зміна).

Функції та завдання підрозділу технічного обслуговування програмно-технічного комплексу Центру:

– організація експлуатації та технічного обслуговування програмно-технічного комплексу Центру;

– підтримка електронного інформаційного ресурсу Центру;

– адміністрування засобів програмно-технічного комплексу Центру;

– участь у впровадженні та забезпеченні функціонування комплексної системи захисту інформації;

– ведення журналів аудиту подій, що реєструються засобами програмно-технічного комплексу Центру;

– встановлення та налагодження програмного забезпечення системи резервного копіювання;

– формування та ведення резервних копій загальносистемного та спеціального програмного забезпечення програмно-технічного комплексу;

– забезпечення актуальності еталонних, архівних і резервних копій реєстрів сертифікатів, що створюються в Центрі, їх зберігання.

Відокремлені пункти реєстрації

До складу відокремлених пунктів реєстрації входять:

– оператор реєстрації (діловод);

– адміністратор реєстрації.

Функції та завдання відокремлених пунктів реєстрації:

– встановлення осіб, які звернулися до Центру з метою формування сертифіката;

– перевірка даних, обов'язкових для формування сертифіката, а також даних, які вносяться в сертифікат на вимогу Абонента;

– укладення договорів про надання послуг ЕЦП;

– ведення реєстрації Абонентів (заявників);

– отримання від Абонентів заявок на формування, скасування, блокування та поновлення сертифікатів ключів;

– надання допомоги Абонентам під час генерації особистих і відкритих ключів у разі отримання від них відповідного звернення та вжиття заходів щодо забезпечення безпеки інформації під час генерації;

– перевірка законності звернень про блокування, поновлення та скасування сертифікатів;

– надання Абонентам консультацій щодо умов і порядку надання послуг електронного цифрового підпису;

– представництво інтересів Центру у відповідному регіоні.

9.7. РОБОТА ІЗ СЕРТИФІКАТАМИ ТА СПИСКАМИ СЕРТИФІКАТІВ

При отриманні послуг ЕЦП Абонентам Центру надаються засоби електронного цифрового підпису, за допомогою яких здійснюється накладання та перевірка ЕЦП, генерація ключів та управління ними, робота з каталогами сертифікатів тощо.

Однією з обов'язкових умов при дорівнюванні ЕЦП до власноручного підпису (печатки) є підтвердження підпису з використанням посиленого сертифіката ключа за допомогою надійних засобів цифрового підпису [5, 6].

У п. 2 постанови Кабінету Міністрів України від 28.10.2004 № 1452 «Про затвердження Порядку застосування електронного цифрового підпису органами державної влади, органами місцевого самоврядування, підприємствами, установами та організаціями державної форми власності» визначено, що державна установа застосовує цифровий підпис лише за умови використання надійних засобів ЕЦП, що повинне бути підтверджено сертифікатом відповідності або позитивним висновком за результатами державної експертизи у сфері криптографічного захисту інформації, отриманим на ці засоби від спеціально уповноваженого центрального органу виконавчої влади у сфері криптографічного захисту інформації, та наявності посилених сертифікатів відкритих ключів у своїх працівників-підписувачів.

На рис. 9.7 наведено головне меню одного з найбільш розповсюдженого в системі ЕЦП України програмного засобу, що має позитивний експертний висновок та забезпечує виконання таких функцій:

– управління ключами підписувача;

– доступ до сертифікатів АЦСК, серверів АЦСК, сертифікатів інших користувачів і списку відкликаних сертифікатів (СВС);

– перевірку чинності та цілісності сертифікатів;

– підпис файлів;

– перевірку ЕЦП файлів;

– зашифрування файлів;

– розшифрування файлів;

– формування позначки часу, взаємодію із захищеними носіями ключової інформації тощо.

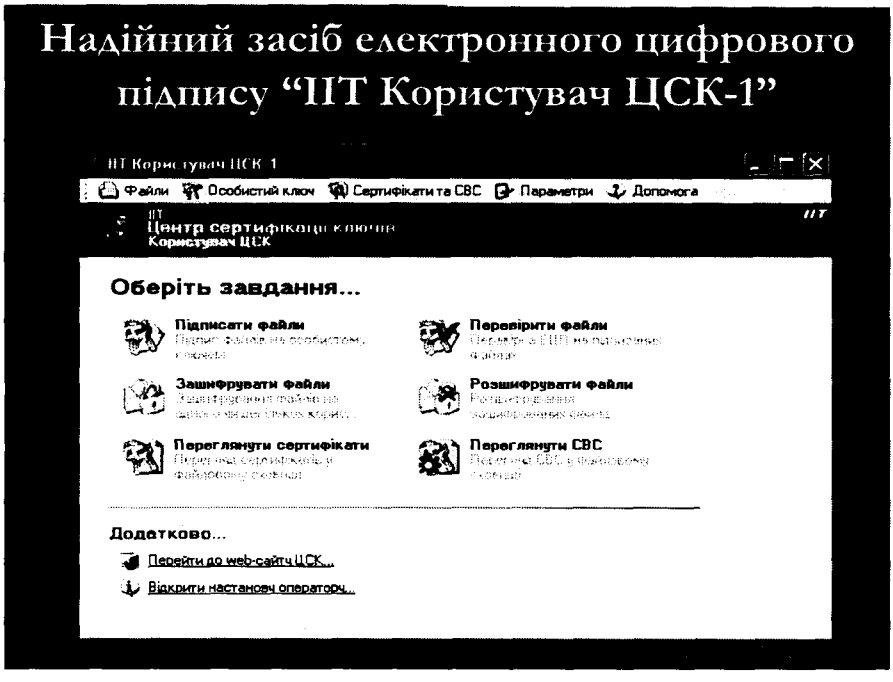

Рис 9.7. Головне меню надійного засобу ЕЦП «ІІТ Користувач ЦСК-1»

Зазначене програмне забезпечення належить до засобів криптографічного захисту інформації виду «Б», які на конструктивному, алгоритмічному та програмному рівнях є єдиними виробами та призначені для використання у складі комплексів обробки та передавання інформації.

Це дозволяє досить просто використовувати такі надійні засоби в складі існуючих та перспективних СЕДО, що практично було підтверджено під час інтеграції цього засобу до систем «АСКОД», «Мегаполіс», «ДІЛО», «Foss-Doc», систем електронної пошти IBM Lotus Notes, Microsoft Outlook, FOSS Mail, системи подання електронної звітності «Інтес QD», «Бест-Звіт», «MD Office», «Сфера-КС» тощо.

Розглянемо більш детально основні функції надійного засобу ЕЦП «ІІТ Користувач ЦСК-1» (далі – програма).

9.7.1. Зчитування сертифікатів і списків відкритих сертифікатів (СВС)

Програма використовує сертифікати та СВС, що зчитуються з файлового сховища при запуску програми. При внесенні змін до файлового сховища під час роботи програми, якщо не встановлено параметр роботи «Автоматично перечитувати файлове сховище при виявленні змін», необхідно перечитати файлове сховище в автоматичному режимі. Для цього необхідно натиснути пункт меню «Зчитати сертифікати та СВС» у розділі меню «Сертифікати та СВС» або натиснути клавішу F9.

9.7.2. Перегляд сертифікатів

Для перегляду сертифікатів, що були зчитані з файлового сховища під час останнього перечитування цього файлового сховища (за замовчанням – при запуску програми), необхідно натиснути «Переглянути сертифікати», натиснути пункт меню «Переглянути сертифікати...» у розділі меню «Сертифікати та СВС» або натиснути клавішу F10.

Вікно перегляду сертифікатів дозволяє видаляти файли сертифікатів з файлового сховища, видаляти сертифікати зі списку сертифікатів, перевіряти сертифікати та переглядати сертифікати. Сертифікати можна відсортувати за типом власника (сертифікати користувачів, сертифікати серверів ЦСК тощо), для цього необхідно натиснути на запис про відповідний тип власника у лівій частині вікна.

Для перегляду сертифіката необхідно натиснути на відповідному записі про сертифікат.

Для видалення файлу сертифіката з файлового сховища або зі списку сертифікатів необхідно виділити відповідний запис про сертифікат і натиснути кнопку «Видалити».

Для перевірки сертифіката необхідно виділити відповідний запис про сертифікат та натиснути кнопку «Перевірити». Перевірка сертифіката здійснюється відповідно до встановлених параметрів роботи, за допомогою OCSP-протоколу, списків відкликаних сертифікатів тощо.

9.7.3. Перегляд СВС

Для перегляду списків відкликаних сертифікатів (СВС), що були зчитані з файлового сховища під час останнього перечитування цього файлового сховища (за замовчанням – при запуску програми), необхідно натиснути «Переглянути СВС» у головному вікні програми, натиснути пункт меню «Переглянути СВС...» у розділі меню «Сертифікати та СВС» або натиснути клавішу F11.

Вікно перегляду СВС дозволяє видаляти файли СВС з файлового сховища, переглядати СВС, завантажувати файли СВС з web-сервера ЦСК або з LDAP-сервера.

Для перегляду СВС необхідно натиснути на відповідному записі про СВС.

Для видалення файлу СВС з файлового сховища необхідно виділити відповідний запис про СВС та натиснути кнопку «Видалити».

9.7.4. Завантаження СВС

Для завантаження списку відкликаних сертифікатів з LDAP-сервера необхідно натиснути «Завантажити СВС» на панелі «Інші завдання...» або пункт меню «Завантажити СВС» у розділі меню «Сертифікати та СВС», а потім натиснути «Завантажити з LDAP-сервера». Якщо всі параметри в «Параметрах роботи» були встановлені правильно, буде здійснено завантаження СВС із LDAP-сервера.

Для завантаження списку відкликаних сертифікатів з web-сервера необхідно натиснути «Завантажити з web-сервера». Якщо всі параметри в «Параметрах роботи» були встановлені правильно, буде здійснено завантаження СВС з web-сервера.

9.7.5. Блокування власного сертифіката

Для блокування власного сертифіката необхідно натиснути пункт меню «Заблокувати власний сертифікат» у розділі меню «Сертифікати та СВС» або натиснути посилання «Заблокувати сертифікат» на панелі «Додаткові завдання». Після цього буде виведене діалогове вікно, у якому необхідно підтвердити необхідність блокування власного сертифіката.

Наступним кроком є зчитування особистого ключа та сертифіката. Необхідно вказати тип носія з особистим ключем, назву носія з особистим ключем, пароль захисту особистого ключа та, за необхідністю (для захищених носіїв ключової інформації – «електронних ключів»), пароль доступу до ключового носія. Також вказується необхідність зчитування особистого ключа при кожній операції; якщо параметр не встановлено, ключ буде зберігатись у пам'яті ПЕОМ під час роботи програми. Щоб особистий ключ зчитувався при кожній операції, необхідно встановити параметр «Зчитувати повторно при кожній операції».

Після зчитування особистого ключа почне роботу майстер блокування сертифіката. Для переходу до наступного вікна необхідно натиснути «Далі».

У наступному вікні майстра блокування сертифіката буде відображено запит на блокування сертифіката (для перевірки візуальної перевірки користувачем

сертифіката, що блокується). Для переходу до наступного вікна необхідно натиснути «Далі».

У наступному вікні майстра блокування сертифіката необхідно обрати сертифікат сервера обробки запитів, до якого буде відправлено запит. Для переходу до наступного вікна необхідно натиснути «Ок».

У наступному вікні майстра блокування сертифіката необхідно обрати спосіб передачі запиту до сервера обробки запитів. Запит може бути переданий через сервер взаємодії ЦСКА протоколом http, електронною поштою або збережений до файлу для відправки іншим способом. Для переходу до наступного вікна необхідно натиснути «Далі».

У наступному вікні необхідно ввести параметри підключення до сервера взаємодії ЦСК: DNS-ім'я чи IP-адресу сервера, TCP-порт, та, за необхідністю, параметри доступу до proxy-сервера (якщо вони не встановлювались у параметрах роботи). Після встановлення параметрів необхідно натиснути «Відправити». Якщо запит було відправлено й оброблено сервером обробки запитів, то робота вважається завершеною.

9.8 РОБОТА З ОСОБИСТИМ КЛЮЧЕМ

9.8.1. Зчитування особистого ключа

Для роботи з деякими функціями програми (шифрування, підпис файлів, робота із сертифікатом) необхідно зчитати особистий ключ користувача. Для зчитування особистого ключа необхідно натиснути пункт меню «Зчитати...» у розділі меню «Особистий ключ» або натиснути комбінацію клавіш Ctrl+K. На виведеному вікні необхідно вказати тип носія з особистим ключем, назву носія з особистим ключем, пароль захисту особистого ключа, та, за необхідністю, (для електронних ключів) пароль доступу до ключового носія. Також вказується необхідність зчитування особистого ключа при кожній операції; якщо параметр не встановлено, ключ буде зберігатись у пам'яті ПЕОМ під час роботи програми. Щоб особистий ключ зчитувався при кожній операції, необхідно встановити параметр «Зчитувати повторно при кожній операції».

9.8.2. Генерація особистого ключа

Для генерації особистого ключа необхідно натиснути пункт меню «Згенерувати ключі» у розділі меню «Особистий ключ» або натиснути посилання «Згенерувати ключі» на панелі «Інші завдання...». Для переходу до наступного вікна необхідно натиснути «Далі».

У наступному вікні майстра генерації ключів необхідно вказати тип криптографічних алгоритмів і протоколів та місце розміщення параметрів криптографічних алгоритмів і протоколів. За замовчанням тип криптографічних алгоритмів та протоколів встановлено «ДСТУ 4145-2004 (ГОСТ 34311-95) та Д-Г в гр. точок ЕК (ГОСТ 28147-89)». Параметри подаються у вигляді dat-файлу та за замовчанням встановлюються до каталогу інсталяції програми. За необхідністю, тип криптографічних алгоритмів і параметри можуть змінюватись.

У наступному вікні майстра генерації ключів необхідно вказати тип ключового носія, назву носія, пароль захисту особистого ключа, та, за необхідністю (для електронних ключів), пароль доступу до ключового носія. Ключові носії можуть бути таких типів: гнучкі диски 3,5 (дискети), з'ємні диски (Flash-диски), оптичні диски (CD-R, CD-RW, DVD-R або DVD-RW), електронні ключі (Кристал, Алмаз, UAToken, AladdineToken R2, PRO, Актив ruToken та інші). Пароль доступу може встановлюватись лише для електронних ключів та не має особливих вимог щодо структури. Пароль захисту особистого ключа повинен відповідати таким вимогам:

1) довжина – не менше 8 символів;

2) не повинен містити однакові символи;

3) не повинен містити підряд більш ніж 2 символи з розкладинки клавіатури;

4) дозволені символи – 'a–z', 'A–Z', '0–9', '+', '–'.

Для отримання допомоги щодо заповнення полів форми вікна «Запис особистого ключа на носій ключової інформації» необхідно натиснути кнопку «Допомога». У наступному вікні майстра генерації ключів необхідно вказати ім'я файлу для запису простого запиту на формування сертифіката у файл. Запит повинен бути записаний на інший носій, ніж особистий ключ. Запит передається до пункту реєстрації Центру для отримання сертифіката.

Після цього майстер завершує свою роботу.

9.8.3. Резервне копіювання особистого ключа

Особистий ключ повинен зберігатись у декількох копіях. Для резервного копіювання особистого ключа необхідно натиснути пункт меню «Резервне копіювання особистого ключа» у розділі меню «Особистий ключ» або натиснути посилання «Резервне копіювання особистого ключа» на панелі «Інші завдання...». Для переходу до наступного вікна необхідно натиснути «Далі».

У наступному вікні майстра резервного копіювання ключів необхідно вказати тип ключового носія та назву носія, з якого буде виконуватись копіювання особистого ключа. Для переходу до наступного вікна необхідно натиснути «Далі».

У наступному вікні майстра резервного копіювання ключів необхідно вказати тип ключового носія та назву носія, до якого буде виконуватись копіювання особистого ключа. Для переходу до наступного вікна необхідно натиснути «Далі».

Далі майстер завершує свою роботу.

9.8.4. Зміна паролю захисту особистого ключа

Для зміни паролю необхідно натиснути пункт меню «Змінити пароль захисту особистого ключа» у розділі меню «Особистий ключ» або натиснути посилання «Змінити пароль захисту особистого ключа» на панелі «Інші завдання...». У формі заміни особистого ключа необхідно встановити тип ключового носія, назву носія, вказати діючий пароль захисту особистого колюча та внести новий пароль захисту особистого ключа з підтвердженням.

9.8.5. Знищення особистого ключа на носії

Ключові дані (особистий ключ) на ключовому носії повинні знищуватись спеціальними засобами. Для знищення особистого ключа необхідно натиснути пункт меню «Знищити особистий ключ на носієві ключової інформації» у розділі меню «Особистий ключ» або натиснути посилання «Знищити особистий ключ» на панелі «Інші завдання...». У формі необхідно встановити тип ключового носія, назву носія та натиснути «Виконати».

9.8.6. Знищення особистого ключа в пам'яті ПЕОМ

Якщо при зчитуванні особистого ключа не було встановлено параметр «Зчитувати повторно при кожній операції», ключ залишається у пам'яті до завершення роботи програми. Якщо необхідно знищити ключ з пам'яті ЕОМ не виходячи з програми, необхідно натиснути пункт меню «Знищити особистий ключ у пам'яті» в розділі меню «Особистий ключ» або натиснути клавішу F12.

9.9. РОБОТА З ФАЙЛАМИ

9.9.1 Підпис файлів

Підпис (накладання ЕЦП) здійснюється на особистому ключі. Для підпису файлу (накладання ЕЦП) необхідно натиснути «Підписати файли» у головному вікні програми, або пункт меню «Підписати» у розділі меню «Файли», або натиснути клавішу F5. Далі потрібно ввести необхідні параметри та натиснути «Зчитати».

Форма містить такі параметри:

– ім'я файлу;

– параметр запису ЕЦП у зовнішньому файлі;

– параметр використання окремого каталогу для підписаних даних чи файлів з ЕЦП;

– каталог для запису підписаних даних чи файлів з ЕЦП.

Параметр «Ім'я файлу» містить імена файлів, що необхідно підписати. Файли додаються до списку файлів за допомогою кнопки «Додати» та стандартного діалогового вікна ОС. Для видалення файлів зі списку необхідно виділити відповідні файли та натиснути «Видалити».

Параметр запису ЕЦП у зовнішньому файлі встановлює необхідність запису ЕЦП до окремого файлу з розширенням «p7s». За замовчанням підпис записується до вихідного файлу та до розширення файлу додається «.p7s». Запис ЕЦП до зовнішнього файлу потрібен у разі, якщо файл підписується декількома користувачами, або за необхідності доступу до структури (вмісту) файлу без зняття з нього ЕЦП.

Параметр використання окремого каталогу для підписаних даних чи файлів з ЕЦП встановлює необхідність запису підписаних файлів або файлів з ЕЦП до окремого каталогу, що задається параметром «Каталог для запису підписаних даних чи файлів з ЕЦП».

Після здійснення підпису файлів виводиться наступне вікно з інформацією про результати підпису.

9.9.2. Перевірка підпису

Для перевірки ЕЦП файлів необхідно натиснути «Перевірити файли» у головному вікні програми, або пункт меню «Перевірити підпис» у розділі меню «Файли», або натиснути клавішу F9. Форма містить такі параметри:

Файли, які необхідно перевірити;

– параметр використання окремого каталогу для файлів без ЕЦП;

– каталог для запису файлів без ЕЦП.

– параметр «Ім'я файлу» містить імена файлів, які необхідно перевірити. Файли додаються до списку файлів за допомогою кнопки «Додати» та стандартного діалогового вікна ОС. Для видалення файлів зі списку необхідно виділити відповідні файли та натиснути «Видалити».

– параметр використання окремого каталогу для файлів без ЕЦП встановлює необхідність запису файлів без ЕЦП до окремого каталогу, що задається параметром «Каталог для запису файлів без ЕЦП».

Для початку перевірки підпису файлів необхідно натиснути «Перевірити». Після перевірки підпису буде виведено інформацію про перевірку. У разі вдалої перевірки буде виведено також інформацію про користувача, що здійснив підпис файлу. Якщо ЕЦП містився у файлі з даними, при перевірці підпису буде створено копію файлу без підпису. За замовчанням (якщо не встановлено окремого каталогу для файлів без підпису) файл буде записаний до того ж каталогу, у якому знаходився підписаний файл.

9.9.3. Шифрування файлів

Для шифрування файлів використовується особистий ключ користувача, що виконує шифрування та сертифікат користувача, для якого шифрується файл. Для шифрування файлу необхідно натиснути «Зашифрувати файли» у головному вікні програми, або пункт меню «Зашифрувати» у розділі меню «Файли», або натиснути клавішу F7. Далі, якщо особистий ключ ще не було зчитано, у вікні потрібно ввести необхідні параметри та натиснути «Зчитати».

Форма містить такі параметри:

– ім'я файлу;

– параметр накладання підпису;

– параметр використання окремого каталогу для зашифрованих файлів;

– каталог для запису зашифрованих файлів.

Параметр «Ім'я файлу» містить імена файлів, що необхідно зашифрувати. Файли додаються до списку файлів за допомогою кнопки «Додати» і стандартного діалогового вікна ОС. Для видалення файлів зі списку необхідно виділити відповідні файли та натиснути «Видалити».

Параметр накладання підпису («Додатково підписати») встановлює необхідність підпису файлу. За замовчанням здійснюється лише шифрування файлу. Вихідний файл має розширення «p7e».

Параметр використання окремого каталогу для зашифрованих файлів встановлює необхідність запису зашифрованих файлів до окремого каталогу, що задається параметром «Каталог для запису зашифрованих файлів».

Для початку процесу шифрування необхідно натиснути «Зашифрувати».

У вікні необхідно обрати користувачів, для яких виконується шифрування файлу. Зашифрований файл може бути відкритим лише користувачем, для якого виконувалось шифрування.

Після здійснення шифрування файлів буде виведене таке вікно з інформацією про результати шифрування.

9.9.4. Розшифрування файлів

Для розшифрування файлів необхідно натиснути «Розшифрувати файли» у головному вікні програми, або пункт меню «Розшифрувати» у розділі меню «Файли», або натиснути клавішу F8. Форма містить такі параметри:

Файли, які необхідно розшифрувати;

– параметр використання окремого каталогу для розшифрованих файлів;

– каталог для запису розшифрованих файлів.

– параметр «Ім'я файлу» містить імена файлів, що необхідно розшифрувати. Файли додаються до списку файлів за допомогою кнопки «Додати» і стандартного діалогового вікна ОС. Для видалення файлів зі списку необхідно виділити відповідні файли та натиснути «Видалити».

Параметр використання окремого каталогу для розшифрованих файлів встановлює необхідність запису розшифрованих файлів до окремого каталогу, що задається параметром «Каталог для запису розшифрованих файлів».

Для початку розшифрування файлів необхідно натиснути «Розшифрувати». Після розшифрування буде виведено інформацію про результати розшифрування. У разі вдалого розшифрування буде виведено також інформацію про користувача, що здійснив шифрування файлу. За замовчанням (якщо не встановлено окремого каталогу для розшифрованих файлів) розшифрований файл буде записаний до того ж каталогу, у якому знаходився зашифрований файл.

9.10. ІНШІ ЗАВДАННЯ

9.10.1. Встановлення параметрів

Встановлення параметрів роботи програми виконується за такими напрямами:

Настроювання параметрів

Для настроювання параметрів роботи програми необхідно натиснути пункт меню «Параметри» або посилання «Встановити параметри» на панелі «Інші завдання...» головного меню програми;

Файлове сховище

Для настроювання параметрів файлового сховища сертифікатів і СВС необхідно у лівій частині вікна «Параметри роботи» натиснути кнопку «Файлове схо-

вище» або кнопку «Далі >» на сторінці настроювання загальних параметрів для переходу до сторінки з формою настроювання параметрів файлового сховища. На сторінці «Файлове сховище» встановлюються такі параметри роботи програми:

Каталог із сертифікатами та СВС

Цей параметр встановлює каталог для файлового сховища сертифікатів та СВС.

Автоматично перечитувати файлове сховище при виявленні змін

Цей параметр визначає необхідність автоматичного перечитування каталогу файлового сховища програмою при внесенні будь-яких змін користувачем до цього каталогу. Якщо параметр не встановлено, необхідно виконувати зчитування каталогу натисканням пункту меню «Зчитати сертифікати та СВС» у розділі меню «Сертифікати та СВС» або натисканням клавіші F9.

Використовувати СВС тільки свого ЦСК

Цей параметр визначає необхідність використовувати при перевірці сертифікатів СВС програму лише свого ЦСК.

Перевіряти наявність двох діючих СВС (повного та часткового)

Цей параметр визначає необхідність перевірки наявності двох діючих СВС (повного та часткового) при здійсненні перевірки сертифікатів. При відключеному параметрі достатньо лише одного діючого СВС.

Якщо параметри були встановлені неправильно або необхідно відмінити настроювання, треба натиснути «Встановити за замовчанням». Для переходу до попередньої сторінки необхідно натиснути «< Назад», для переходу до наступної сторінки необхідно натиснути «Далі >»;

Proksy-сервер

Для настроювання параметрів proxy-сервера необхідно у лівій частині вікна «Параметри роботи» натиснути кнопку «Proxy-сервер» або кнопку «Далі >» на сторінці настроювання файлового сховища (або іншої попередньої сторінки) для переходу до сторінки з формою настроювання параметрів proxy-сервера. На сторінці «Proxy-сервер» встановлюються такі параметри роботи програми:

Ім'я чи IP-адреса сервера. Цей параметр встановлює IP-адресу або DNS-ім'я proxy-сервера.

TCP-порт. Цей параметр встановлює TCP-порт proxy-сервера.

Ім'я користувача. Цей параметр встановлює ім'я користувача proxy-сервера.

Пароль. Цей параметр встановлює пароль користувача proxy-сервера.

Зберегти пароль. Цей параметр встановлює необхідсть зберігати пароль доступу до proxy-сервера в програмі.

Якщо параметри були встановлені неправильно або необхідно відмінити настроювання, треба натиснути «Встановити за замовчанням». Для переходу до попередньої сторінки необхідно натиснути «< Назад», для переходу до наступної сторінки необхідно натиснути «Далі >»;

TSP-сервер

Для настроювання параметрів TSP-сервера необхідно у лівій частині вікна «Параметри роботи» натиснути кнопку «TSP-сервер» або кнопку «Далі >» на

сторінці настроювання proxy-сервера (або іншої попередньої сторінки) для переходу до сторінки з формою настроювання параметрів TSP-сервера. На сторінці «TSP-сервер» встановлюються такі параметри роботи програми:

Ім'я чи IP-адреса сервера. Цей параметр встановлює IP-адресу або DNS-ім'я TSP-сервера.

TCP-порт. Цей параметр встановлює TCP-порт TSP-сервера.

Ці параметри можна встановити із сертифіката TSP-сервера або із сертифіката ЦСК. Для цього необхідно натиснути «Встановити із сертифіката». При цьому адреса (або ім'я TSP-сервера) буде отримана із сертифіката цього сервера, а за його відсутністю – із сертифіката ЦСК.

Якщо параметри були встановлені неправильно або необхідно відмінити настроювання, треба натиснути «Встановити за замовчанням». Для переходу до попередньої сторінки необхідно натиснути «< Назад», для переходу до наступної сторінки необхідно натиснути «Далі >»;

OCSP-сервер

Для настроювання параметрів OCSP-сервера необхідно у лівій частині вікна «Параметри роботи» натиснути кнопку «OCSP-сервер» або кнопку «Далі >» на сторінці настроювання TSP-сервера (або іншої попередньої сторінки) для переходу до сторінки з формою настроювання параметрів OCSP-сервера. На сторінці «OCSP-сервер» встановлюються такі параметри роботи програми:

Ім'я чи IP-адреса сервера. Цей параметр встановлює IP-адресу або DNS-ім'я OCSP-сервера.

TCP-порт. Цей параметр встановлює TCP-порт OCSP-сервера.

Перевіряти статус сертифікатів через OCSP до перевірки у файловому сховищі. Цей параметр встановлює черговість перевірки статусу сертифіката, що використовується. Якщо параметр встановлено, статус сертифіката перевіряється спочатку за допомогою OCSP-протоколу, потім за допомогою сертифікатів (списків відкликаних сертифікатів) з локального файлового сховища (якщо встановлено параметр використання CBC з файлового сховища для перевірки статусу сертифікатів). Якщо параметр не встановлено, перевірка здійснюється спочатку за допомогою сертифікатів (списків відкликаних сертифікатів) з файлового сховища, а потім (за необхідністю) – за допомогою OCSP-протоколу.

Параметри (ім'я чи IP-адреса сервера та TCP-порт) можна встановити із сертифіката OCSP-сервера або із сертифіката ЦСК. Для цього необхідно натиснути «Встановити із сертифіката». При цьому адреса (або ім'я OCSP-сервера) буде отримана із сертифіката цього сервера, а за його відсутністю – із сертифіката ЦСК.

Якщо параметри були встановлені неправильно або необхідно відмінити настроювання, треба натиснути «Встановити за замовчанням». Для переходу до попередньої сторінки необхідно натиснути «< Назад», для переходу до наступної сторінки необхідно натиснути «Далі >»;

LDAP-сервер

Для настроювання параметрів LDAP-сервера необхідно в лівій частині вікна «Параметри роботи» натиснути кнопку «LDAP-сервер» або кнопку «Далі >» на сторінці настроювання OCSP-сервера (або іншої попередньої сторінки) для пере-

ходу до сторінки з формою настроювання параметрів LDAP-сервера. На сторінці «LDAP-сервер» встановлюються такі параметри роботи програми:

Ім'я чи IP-адреса сервера. Цей параметр встановлює IP-адресу або DNS-ім'я LDAP-сервера.

TCP-порт. Цей параметр встановлює TCP-порт LDAP-сервера.

Анонімний доступ. Цей параметр встановлює порядок доступу до LDAP-сервера без використання імені користувача та паролю (встановлюється за замовчанням).

Ім'я користувача. Цей параметр використовується, якщо не встановлено параметр «анонімний доступ» та встановлює ім'я користувача при доступі до LDAP-сервера.

Пароль доступу. Цей параметр використовується якщо не встановлено параметр «анонімний доступ» та встановлює пароль при доступі до LDAP-сервера.

Шукати сертифікати у LDAP-каталозі. Цей параметр встановлює необхідність пошуку сертифікатів у LDAP-каталозі. Якщо параметр не встановлено, доступ до LDAP-каталогу здійснюється лише для завантаження списків відкликаних сертифікатів і сертифікатів у ручному режимі.

Параметр «Ім'я чи IP-адреса сервера» можна встановити із сертифіката ЦСК. Для цього необхідно натиснути «Встановити із сертифіката». При цьому адреса (або ім'я LDAP-сервера) буде отримана із сертифіката ЦСК.

Якщо параметри були встановлені неправильно або необхідно відмінити настроювання, треба натиснути «Встановити за замовчанням». Для переходу до попередньої сторінки необхідно натиснути «< Назад». Для завершення настроювань параметрів роботи необхідно натиснути «Готово». Для збереження параметрів без закриття вікна параметрів роботи необхідно натиснути «Застосувати».

9.10.2. Режим роботи з ЦСК

Програма може працювати у двох режимах:

– режим on-line (взаємодія з ЦСК);

– режим off-line (без взаємодії з ЦСК).

У першому режимі програма може передавати запити за допомогою мереж передачі даних до сервера взаємодії ЦСК (TSP-, LDAP- або OCSP-серверів) якщо відповідні параметри встановлені у параметрах роботи.

У другому режимі програма не передає даних за допомогою мереж передачі даних, навіть якщо встановлені параметри серверів ЦСК. Цей режим використовується для роботи без підключення до мереж передачі даних.

Для встановлення режиму роботи з ЦСК необхідно натиснути пункт меню «Режим off-line (без взаємодії з ЦСК)» у розділі меню «Параметри».

9.11. СТАН ЗАСТОСУВАННЯ ТА ПРОБЛЕМНІ ПИТАННЯ РОЗВИТКУ СИСТЕМИ ЕЦП

Як на міжнародному рівні, так і в Україні існує значне число проблемних питань теоретичного та практичного характеру. На наш погляд, найбільш характерними є такі теоретичні питання:

1. Аналіз криптографічної стійкості криптографічних перетворень (стандартів) і безпечності криптографічних механізмів (протоколів) для заданих моделей порушника й загроз та визначення можливостей і умов їх застосування.

2. Удосконалення методів та алгоритмів криптографічних перетворень за критерієм мінімізації складності арифметичних операцій у кільцях, полях, групах точок еліптичних і гіпереліптичних кривих, спарювання точок еліптичних кривих тощо.

3. Теоретичне обґрунтування безпечності та стійкості існуючих і перспективних генераторів випадкових і детермінованих випадкових чисел (послідовностей), подальше їх удосконалення за критерієм мінімізації складності генерування та фільтрації (тестування).

4. Розробка науково-методичного апарату порівняльного аналізу та оцінки криптографічних перетворень і криптографічних протоколів з використанням сукупності умовних і безумовних критеріїв.

5. Удосконалення й розвиток системи стандартизації та сертифікації в плані розробки та гармонізації стандартів криптографічних перетворень і криптографічних механізмів і протоколів.

6. Теоретичні оцінки та прогнозування вимог і умов та обмежень щодо застосування стандартизованих криптографічних примітивів і криптографічних протоколів в умовах розвитку математичних методів і потужностей криптоаналітичних систем.

7. Дослідження та прогнозування розвитку й удосконалення міжнародних ІВК, розроблення політики безпеки та гармонізація національної системи ЕЦП з міжнародними ІВК та ІВК технологічно розвинених держав.

8. Подальше теоретичне обґрунтування вимог та умов надання користувачам послуг ІВК з апаратним (вищим) та середньоапаратним рівнями гарантій, за яких практично виключаються можливості несанкціонованого доступу до особистих (таємних) ключів і до засобів КЗІ.

Практичні проблемні питання розвитку системи ЕЦП в Україні

На наш погляд, найбільш характерними є такі практичні проблемні питання.

1. Удосконалення та розвиток нормативно-правового забезпечення щодо національної системи ЕЦП (ІВК) з урахуванням стану й тенденцій розвитку ІВК технологічно розвинених держав і міжнародних ІВК, необхідності нормативно-правового забезпечення національної системи в частині взаємодії з іншими ІВК на міждержавному та міждержавному рівнях.

2. Практичне створення та впровадження програмно-технічних комплексів ЦЗО, які забезпечували б функціонування різних прикладних електронних систем, у першу чергу електронних документів, електронного документообігу, платіжних систем, електронних цифрових паспортів, захищених систем електронної пошти, різної електронної звітності тощо.

3. Затвердження та введення в дію основних технічних специфікацій щодо форматів даних і протоколів взаємодії, у першу чергу, та, на наш погляд, обовязково таких, як [57–60]:

3.1. Національна система електронного цифрового підпису. Технічні специфікації форматів представлення базових об'єктів. Формат підписаних даних.

3.2. Національна система електронного цифрового підпису. Технічні специфікації протоколів взаємодії. Протокол визначення статусу сертифіката.

3.3. Національна система електронного цифрового підпису. Технічні специфікації протоколів взаємодії. Протокол фіксування часу.

3.4. Національна система електронного цифрового підпису. Технічні специфікації форматів криптографічних повідомлень. Захищені дані.

Зрозуміло, що це болючий процес, оскільки різні розробники мають свої погляди відносно механізмів і протоколів, які реалізовані в уже діючих системах. Але це потрібно зробити, тоді ми будемо ближче до міжнародних ІВК.

4. Стандартизація криптографічних примітивів і криптографічних механізмів і протоколів, що використовуються, за можливістю впровадження в національну систему більшості або всіх основних криптопримітивів і криптопротоколів, що є міжнародними стандартами або рекомендовані до застосування.

5. Практичне впровадження на всіх рівнях – від ЦЗО до кінцевого користувача апаратних засобів КЗІ, які забезпечували б вищий рівень гарантій та можливість відображення політики на міжнародному та міждержавному рівнях.

6. Практичне створення економічно обґрунтованої та беззбиткової ІВК, включаючи декілька засвідчувальних центрів і сукупності АЦСК та ЦСК, а також узгоджене впровадження системи відокремлених пунктів, включно до районних адміністративних одиниць.

7. Аналіз і визначення умов довіри до третіх довірчих сторін – ЦЗО, ЗЦ, АЦСК, ЦСК, відокремлених пунктів та інформаційного забезпечення кінцевих користувачів. Необхідно мати на увазі, що системи та засоби порушників будуть безперервно вдосконалюватися та розвиватися, тому повинні розвиватись усі елементи ІВК.

8. Особлива увага має бути приділена питанням підготовки та перепідготовки спеціалістів, що задіяні в обслуговуванні, розробці, проведенні експертизи, веденні відповідної роботи та навчанні користувачів. Підтримання на необхідному рівні навчально-методичного забезпечення функціонування системи ЕЦП, а з часом, ми сподіваємось, ІВК як на внутрішньому, так і міждержавному та міжнародному рівнях.

На рис. 9.8 і 9.9 наведені дані щодо стану нормативно-правового забезпечення системи ЕЦП відносно внутрішніх користувачів і застосувань і стану створення й застосування структурних елементів національної системи. Зрозуміло, що з часом ці дані зміняться, але ми їх наводимо як сьогоднішній факт. На рис. 9.10 наведено всі діючі елементи системи ЕЦП України на початок квітня 2010 року. На рис. 9.11 наведено структурну схему захищеної корпоративної мережі типу «клієнт – сервер». Функціонування та надання послуг з безпеки інформації в них базується на застосуванні для надання послуг третьої довірчої сторони – національної системи ЕЦП. По суті, детально ці системи розглянуті й аналізуються в розділі 6 цієї монографії.

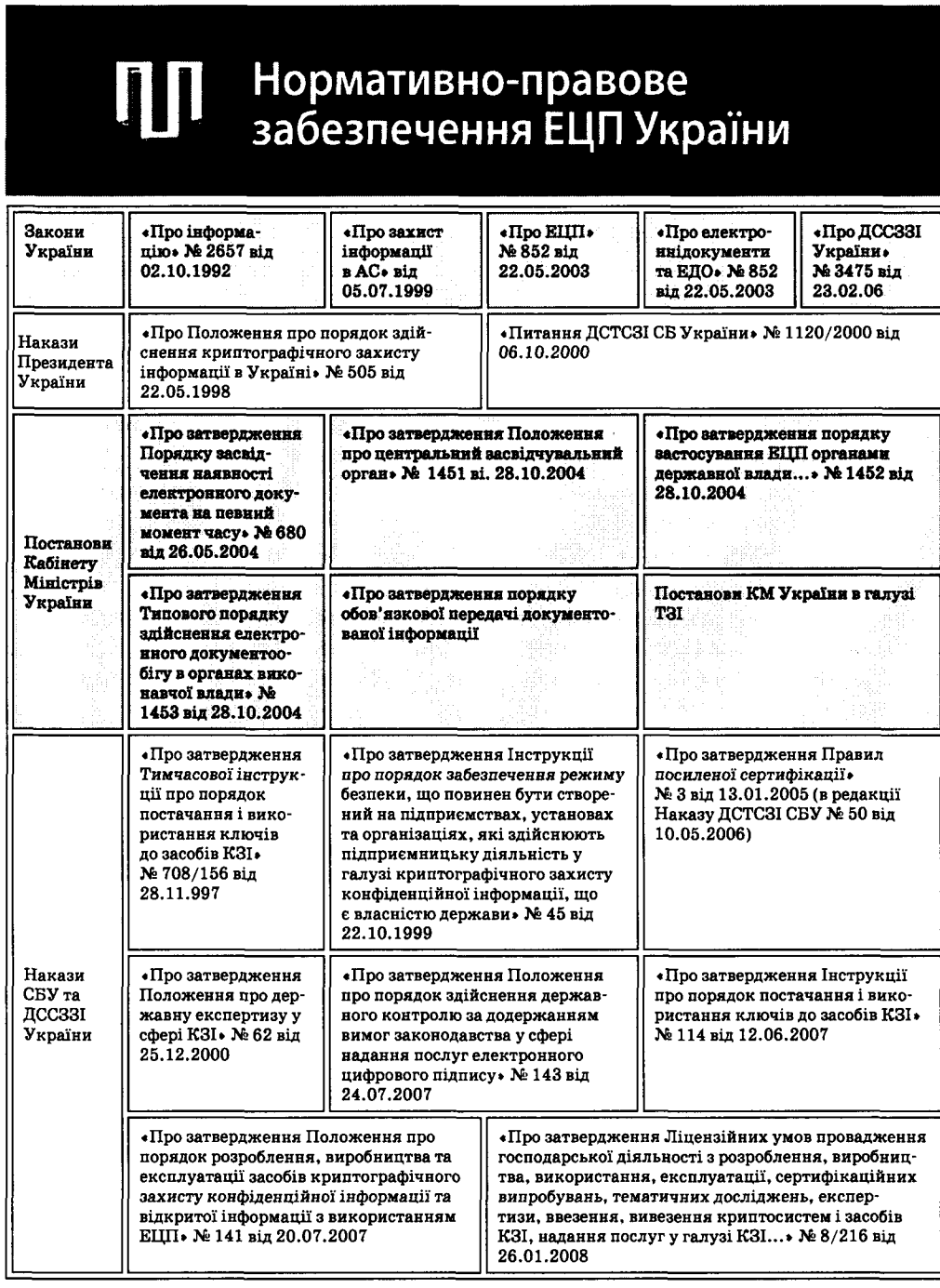

Рис. 9.8. Стан нормативно-правового забезпечення системи ЕЦП України

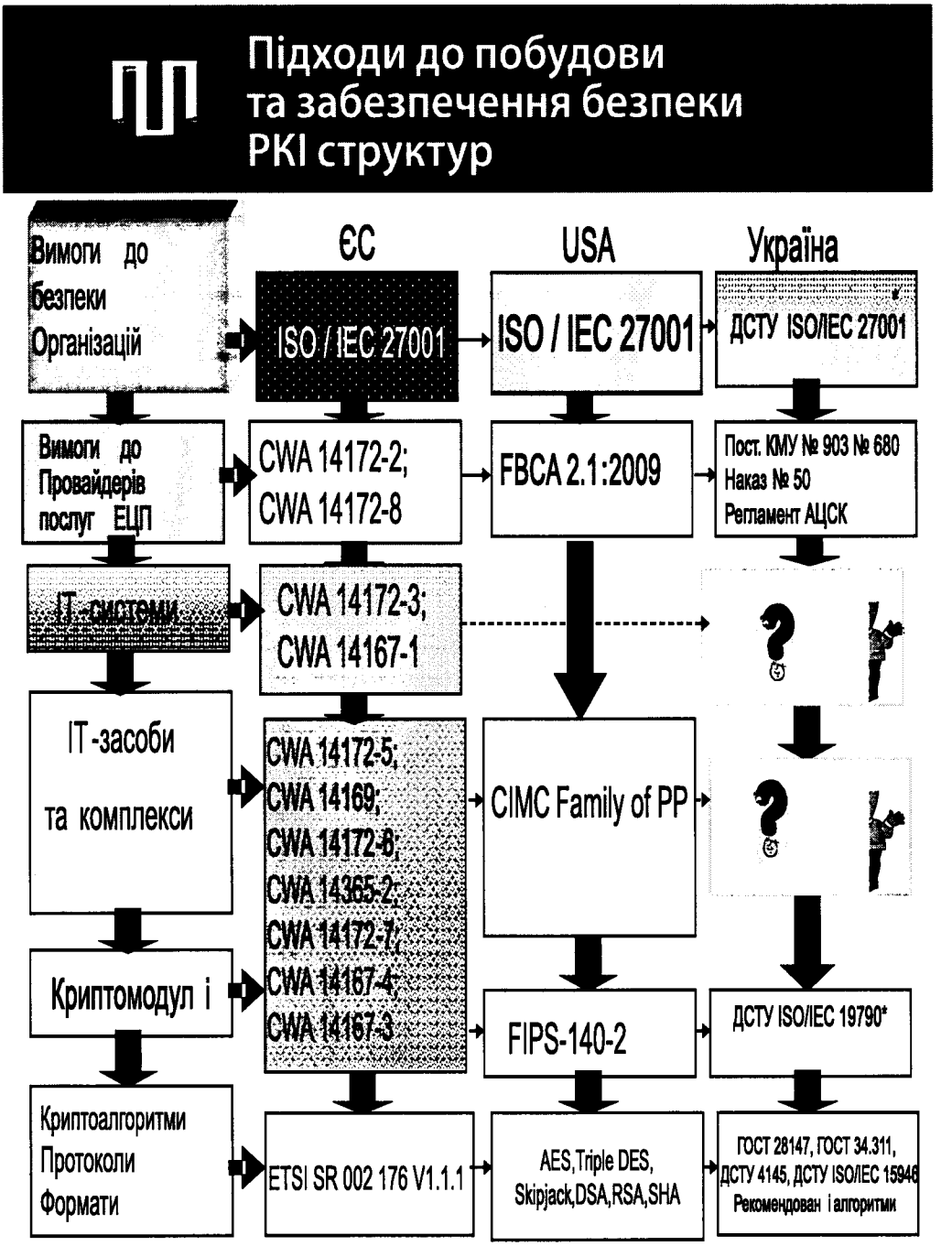

Рис. 9.9. Нормативно-правове забезпечення побудови ІВК в ЄС, США та Україні

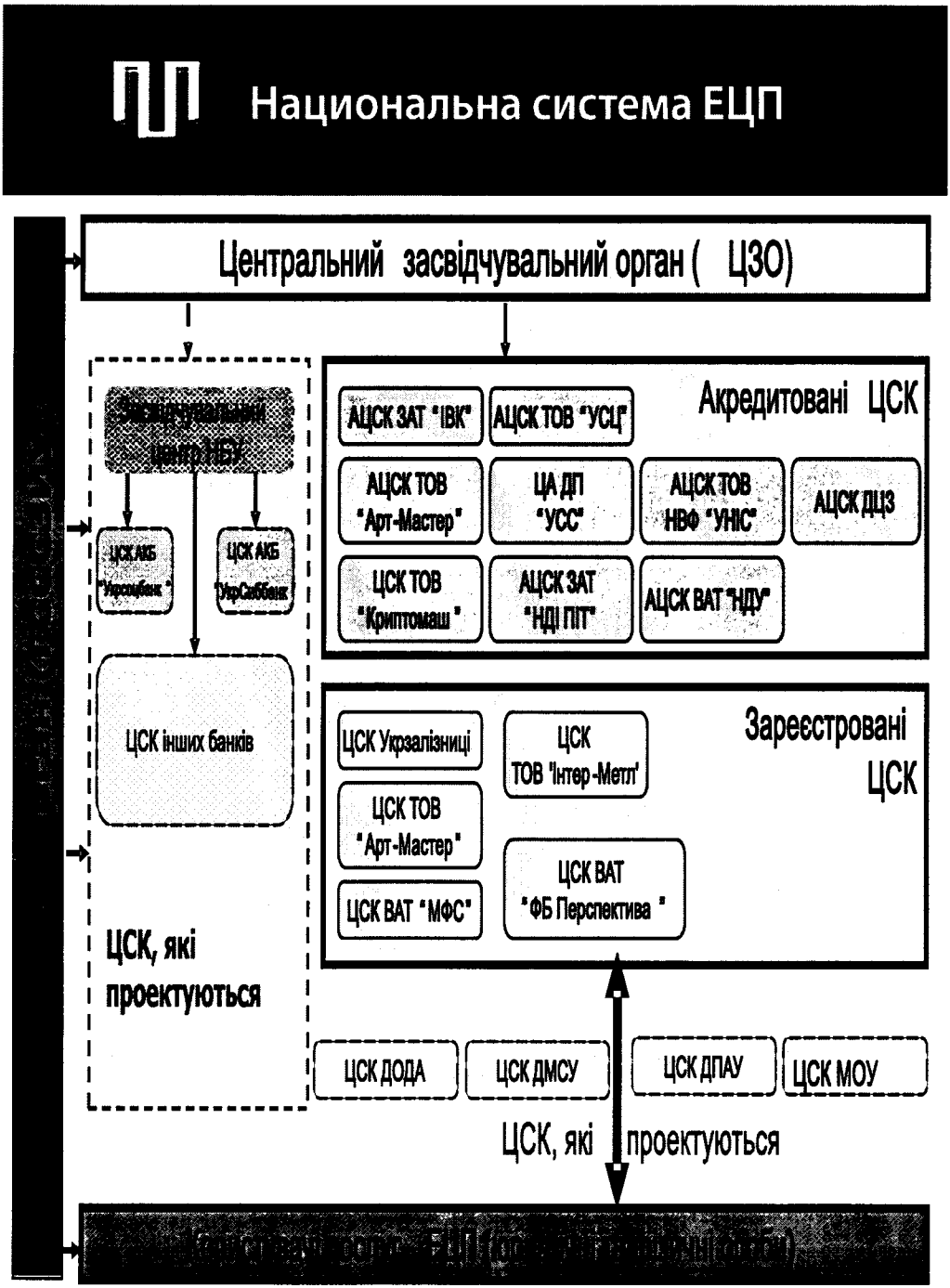

Рис. 9.10. Стан системи ЕЦП України на квітень 2010 року

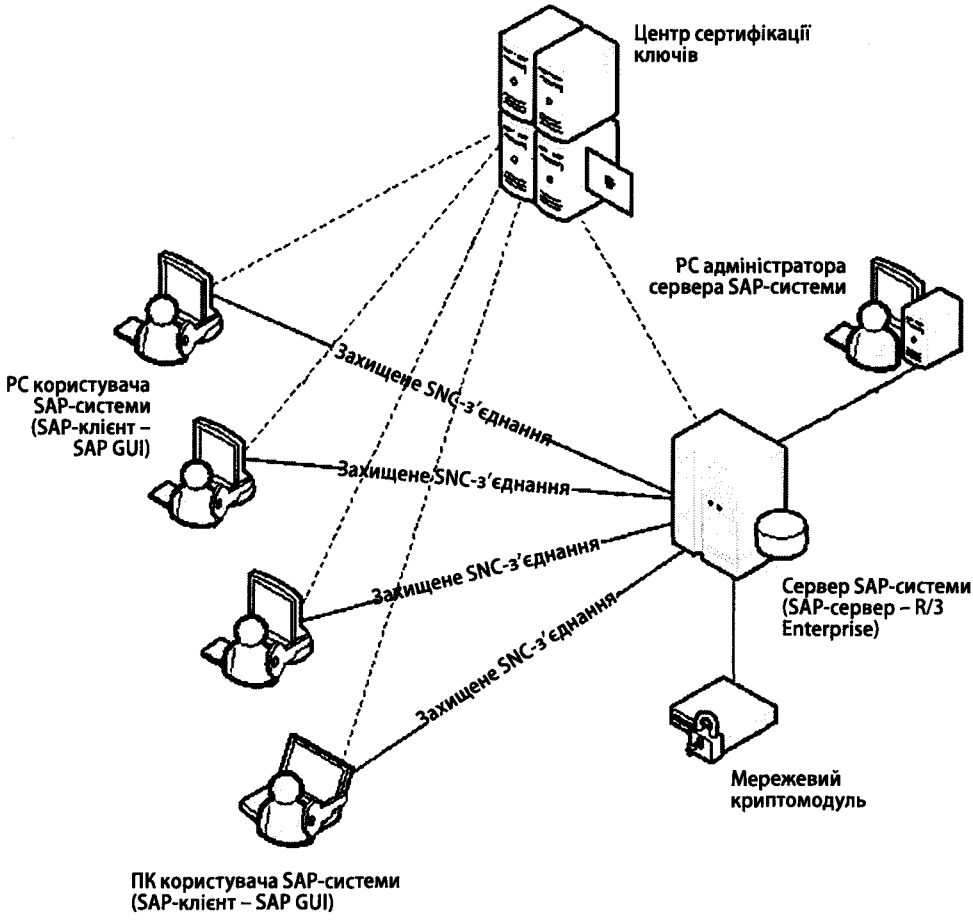

Рис. 9.11. Захищена банківська SAP