



СЛУЖБИ БЕЗПЕКИ УКРАЇНИ
ДЕПАРТАМЕНТ СПЕЦІАЛЬНИХ ТЕЛЕКОМУНІКАЦІЙНИХ
СИСТЕМ ТА ЗАХИСТУ ІНФОРМАЦІЇ

Н А К А З

10.05.2006 N 50

Зареєстровано в Міністерстві
юстиції України
17 травня 2006 р.
за N 568/12442

**Про внесення змін
до Правил посиленої сертифікації**

Відповідно до Порядку акредитації центру сертифікації ключів, затвердженого постановою Кабінету Міністрів України від 13 липня 2004 року N 903 ([903-2004-п](#)), з метою вдосконалення організаційних, технічних і технологічних вимог до акредитованих центрів сертифікації ключів під час обслуговування ними посилених сертифікатів ключів та забезпечення їх використання **Н А К А З У Ю**:

1. Внести зміни до Правил посиленої сертифікації, затверджених наказом Департаменту спеціальних телекомунікаційних систем та захисту інформації Служби безпеки України від 13 січня 2005 року N 3 та зареєстрованих в Міністерстві юстиції України 27 січня 2005 року за N 104/10384 ([z0104-05](#), [za104-05](#)), виклавши їх у новій редакції (додаються).

2. Начальнику Головного управління криптографічного захисту інформації Департаменту спеціальних телекомунікаційних систем та захисту інформації Служби безпеки України забезпечити в установленому порядку подання цього наказу на державну реєстрацію до Міністерства юстиції України.

3. Контроль за виконанням цього наказу покласти на першого заступника начальника Департаменту спеціальних телекомунікаційних систем та захисту інформації Служби безпеки України.

Начальник Департаменту

К.Бойко

ПОГОДЖЕНО:

Голова Держпідприємництва
України

А.В.Дашкевич

**В.о. Голови Антимонопольного
комітету України**
Міністр транспорту та зв'язку
України

С.С.Стефановський

В.В.Бондар

ЗАТВЕРДЖЕНО

Наказ Департаменту спеціальних телекомунікаційних систем та захисту інформації Служби безпеки України 13.01.2005 N 3 (z0104-05)
(у редакції наказу Департаменту спеціальних телекомунікаційних систем та захисту інформації Служби безпеки України від 10.05.2006 N 50)

Зареєстровано в Міністерстві юстиції України 17 травня 2006 р.
за N 568/12442

ПРАВИЛА посиленої сертифікації

1. Загальні положення

1.1. Правила посиленої сертифікації (далі - Правила) розроблені на виконання постанови Кабінету Міністрів України від 13 липня 2004 року N 903 (903-2004-п) "Про затвердження Порядку акредитації центру сертифікації ключів" та визначають організаційні, технічні і технологічні вимоги до акредитованих центрів сертифікації ключів (далі - акредитовані центри) під час обслуговування ними посилених сертифікатів відкритих ключів (далі - сертифікат) та забезпечення їх використання.

1.2. У цих Правилах організаційні, технічні і технологічні умови діяльності акредитованих центрів під час обслуговування ними сертифікатів мають назву політика сертифікації.

1.3. Сертифікати, сформовані відповідно до вимог політики сертифікації, використовуються для підтримки електронного цифрового підпису, який задовольняє вимогам щодо підпису, застосованого до даних в електронній формі, у такий же спосіб, як власноручні підписи задовольняють вимогам стосовно документа на папері.

1.4. Дія цих Правил поширюється на акредитовані центри. Особливості застосування цих Правил у сфері банківської діяльності визначає Національний банк України за погодженням з контролюючим органом.

1.5. Використані у цих Правилах терміни мають такі значення:

автоматизована система акредитованого центру - організаційно-технічна система акредитованого центру, що забезпечує обслуговування сертифікатів та об'єднує програмно-технічний комплекс, фізичне середовище, обслуговуючий персонал, а також інформацію, що обробляється в акредитованому центрі;

відокремлений пункт реєстрації - представництво (філія, підрозділ) акредитованого центру, яке здійснює реєстрацію підписувачів;

захисний носій - носій (smart card, touch-memory тощо), що призначений для зберігання особистого ключа та має вбудовані апаратно-програмні засоби, що забезпечують захист записаних на нього даних від несанкціонованого доступу;

розпізнавальне ім'я - сукупність реквізитів підписувача, що забезпечують можливість однозначного визначення належності сертифіката цьому підписувачу серед інших сертифікатів, сформованих у акредитованому центрі;

заявник - фізична або юридична особа, яка звертається до акредитованого центру з метою формування сертифіката (сертифікатів);

реєстрація - встановлення підписувача та перевірка наданих даних, що включаються у сертифікат;

сертифікація - формування сертифіката, заснованого на перевірених при реєстрації даних, накладання на сертифікат електронного цифрового підпису за допомогою особистого ключа акредитованого центру;

розповсюдження - надання сертифіката підписувачу - власнику особистого ключа або, у разі його згоди, іншим користувачам, якщо для державних органів інше не передбачене правилами їх систем електронного документообігу. Зазначеною послугою також забезпечується розповсюдження інформації щодо умов та порядку обслуговування і використання сертифіката;

управління статусом сертифіката - зміна статусу сертифіката на підставі відповідних запитів та за умовами, визначеними Законом України "Про електронний цифровий підпис" ([852-15](#));

розповсюдження інформації про статус сертифіката - надання вільного доступу до інформації про статус сертифіката. Зазначена послуга може бути забезпечена у реальному часі або заснована на інформації про статус сертифіката, що оновлюється за визначеним періодом часу або у разі необхідності;

повторне формування сертифіката - формування нового сертифіката акредитованим центром для підписувача, який є власником чинного сертифіката, сформованого даним акредитованим центром.

Інші терміни застосовуються у значеннях, наведених у Законі України "Про електронний цифровий підпис" ([852-15](#)), Порядку акредитації центру сертифікації ключів, затвердженому постановою Кабінету Міністрів України від 13 липня 2004 року № 903 ([903-2004-п](#)), інших нормативно-правових актах з питань криптографічного та технічного захисту інформації.

1.6. Заявник та підписувач

1.6.1. У разі, якщо в основних даних (реквізитах) підписувача, сформованого за зверненням заявника сертифіката зазначаються реквізити заявника, заявник та підписувач є одним суб'єктом.

1.6.2. В іншому випадку, якщо заявник - уповноважений представник юридичної особи звертається до акредитованого центру з метою формування сертифікатів для інших представників цієї юридичної особи, заявник та підписувач є різними суб'єктами.

1.6.3. Заявник, який укладає договір із акредитованим центром на надання послуг електронного цифрового підпису (далі - ЕЦП), несе перед ним відповідальність, передбачену договором, за використання особистих ключів, які відповідають сертифікатам, сформованим акредитованим центром за зверненням заявника.

Підписувач здійснює використання особистого ключа відповідно до умов договору.

1.7. Ідентифікатор політики сертифікації

Ідентифікатором для політики сертифікації, що визначена у цих Правилах, є iso(1) member-body(2) Ukraine(804) root(2) security(1) cryptography(1) pk(1) pk-cp(2) правила посиленої сертифікації(2).

Центр сертифікації ключів, що успішно пройшов процедуру акредитації, у процесі якої підтверджено відповідність діяльності центру вимогам, зазначеним у цих Правилах, повинен включати зазначений ідентифікатор у всі посилені сертифікати, що ним формуються для підписувачів.

2. Обов'язки акредитованого центру

2.1. Акредитований центр повинен зобов'язати заявника виконувати такі основні вимоги:

- 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;
- г) негайно інформувати акредитований 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;
- д) не використовувати особистий ключ у разі його компрометації.

2.2. У разі, якщо заявник та підписувач є різними суб'єктами, заявник повинен зобов'язати підписувача виконувати вимоги, визначені у пункті 2.1 цих Правил.

2.3. Акредитований центр зобов'язаний надати користувачам, які використовують сертифікати, інформацію про необхідність:

- здійснення перевірки чинності сертифіката з використанням інформації про статус сертифіката;
- врахування усіх визначених у сертифікаті вимог щодо його використання.

3. Вимоги до діяльності акредитованого центру під час обслуговування сертифікатів

3.1. Акредитований центр повинен мати Регламент роботи, що визначає порядок та процедури обслуговування сертифікатів підписувачів відповідно до вимог, визначених у цих Правилах.

3.2. У Регламенті роботи повинно бути визначено:

- 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 і використанні сертифікатів та їх функції;
- в) сфера використання сертифіката:
 - перелік сфер, у яких дозволяється використання сертифікатів, сформованих акредитованим центром;
 - обмеження щодо використання сертифікатів, сформованих акредитованим центром;
- г) порядок розповсюдження (публікації) інформації акредитованим центром:
 - перелік інформації, що публікується акредитованим центром на електронному інформаційному ресурсі;
 - час і порядок публікації сертифікатів та списків відкликаних сертифікатів;
- г) порядок ідентифікації та автентифікації:

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

умови встановлення юридичної особи (представника юридичної особи) або фізичної особи - підписувачів (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 і скасування) та поновлення сертифіката;

д) умови, процедури та механізми, пов'язані із формуванням, блокуванням, скасуванням та використанням сертифіката:

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 у режимі реального часу);

закінчення строку чинності сертифіката підписувача;

е) 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 у 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 та даних, що підлягають архівуванню, строки зберігання архівів, механізми та порядок зберігання і захисту архівів);

є) управління ключами:

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

процедури надання особистого ключа після генерації акредитованим центром його власнику;

механізм надання відкритого ключа акредитованому центру для сертифікації;

ж) 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.

3.3. Регламент роботи розробляється до початку проведення процедури акредитації центру сертифікації ключів та затверджується керівником центру після його погодження з контролюючим органом.

Після затвердження Регламенту роботи один його примірник надсилається до контролюючого органу.

3.4. У разі внесення змін до Регламенту роботи у ньому окремо зазначаються положення (розділи, пункти), до яких внесено зміни, текст змін, а також дата їх внесення.

Погодження та затвердження змін до Регламенту роботи здійснюються у порядку, встановленому для погодження та затвердження Регламенту роботи.

3.5. Акредитований центр через електронний інформаційний ресурс або в інший спосіб забезпечує ознайомлення користувачів з положеннями Регламенту роботи або з іншими документами, що підтверджують відповідність його діяльності політиці сертифікації, що визначена у цих Правилах. Акредитований центр визначає обсяг положень Регламенту роботи або інших документів, з якими необхідно ознайомлювати користувачів.

4. Управління ключами в акредитованому центрі

4.1. Генерація ключів акредитованого центру

4.1.1. Генерація особистого ключа акредитованого центру повинна здійснюватись у спеціальному приміщенні за участю або під контролем не менше двох визначених осіб із обслуговуючого персоналу. Вимоги до спеціальних приміщень акредитованого центру наведені у додатку до цих Правил.

4.1.2. Генерація ключів акредитованого центру здійснюється за допомогою надійних засобів ЕЦП.

4.1.3. Всі події, пов'язані із генерацією, використанням та знищенням особистого ключа акредитованого центру, повинні протоколюватися.

4.2. Зберігання, резервування та відновлення ключа акредитованого центру

4.2.1. 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 пунктом 4.1.2 цих Правил;

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

4.2.2. У разі здійснення резервування особистого ключа акредитованого центру особистий ключ повинен бути перенесений на зовнішній носій (пристрій) у захищеному вигляді, що забезпечує його цілісність та конфіденційність.

4.2.3. Резервування, зберігання та відновлення особистого ключа повинно здійснюватися у спеціальному приміщенні. Резервування та відновлення здійснюється за участю або під контролем не менше двох визначених осіб із числа обслуговуючого персоналу.

4.2.4. 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.

4.2.5. У разі, якщо ключ зберігається у призначеному для цього програмно-апаратному або апаратному засобі КЗІ, технологія зберігання повинна забезпечити неможливість доступу до нього іззовні у відношенні до такого засобу.

4.3. Використання особистого ключа акредитованого центру

4.3.1. Особистий ключ акредитованого центру може використовуватися тільки для формування сертифікатів (накладання ЕЦП на сертифікат) та інформації про статус сертифіката.

4.3.2. Особистий ключ акредитованого центру може використовуватися тільки у засобах КЗІ, які повинні бути розташовані у спеціальному приміщенні.

4.4. Строк чинності особистого ключа акредитованого центру

4.4.1. Особистий ключ акредитованого центру може бути чинним не більше ніж п'ять років.

4.4.2. Після закінчення терміну дії особистого ключа акредитованого центру особистий ключ та всі його резервні копії знищуються способом, що не дозволяє їх відновлення.

4.5. Надання допомоги із генерації ключів підписувачам

4.5.1. У разі генерації ключів підписувачам акредитований центр повинен вжити заходи конфіденційності під час генерації.

4.5.2. У разі передачі акредитованим центром особистого ключа підписувачу через заявника повинна бути забезпечена конфіденційність та цілісність ключа.

4.5.3. Зберігання особистих ключів підписувачів та ознайомлення з ними в акредитованому центрі забороняються.

4.5.4. Генерація ключів акредитованим центром підписувачам повинна здійснюватися за допомогою надійних засобів ЕЦП.

5. Обслуговування сертифікатів

5.1. Обслуговування акредитованим центром сертифікатів передбачає:

реєстрацію;
сертифікацію;
розповсюдження;
управління статусом сертифіката;
розповсюдження інформації про статус сертифіката.
Додатково акредитований центр може надавати засоби ЕЦП.

5.2. Реєстрація підписувача

5.2.1. Встановлення юридичної особи здійснюється за її установчими документами (положення, статут юридичної особи тощо) або копіями таких документів, які нотаріально посвідчені відповідно до законодавства. Крім цього, акредитований центр встановлює представника юридичної особи та його повноваження.

5.2.2. Встановлення фізичної особи здійснюється за паспортом або іншими документами відповідно до законодавства.

У разі, якщо під час реєстрації встановлюється підписувач - фізична особа як представник юридичної особи, заявник повинен додатково надати до акредитованого центру відомості щодо належності підписувача до цієї юридичної особи.

5.2.3. Заявник повинен надати свою адресу, телефон або іншу інформацію, що дозволяє зв'язатися з ним.

5.2.4. Реєстрація підписувачів може здійснюватися через відокремлені пункти реєстрації, які виконують свої функції згідно з Регламентом роботи.

5.2.5. У разі, якщо особистий та відкритий ключі були згенеровані не акредитованим центром, під час реєстрації повинно бути забезпечено перевірку щодо володіння підписувачем особистим ключем, який відповідає відкритому ключу, наданому для формування сертифіката. Перевірка виконується без розкриття особистого ключа підписувача.

5.2.6. Перед укладенням договору із заявником щодо надання послуг ЕЦП акредитований центр повинен ознайомити заявника із умовами обслуговування сертифікатів, які визначено у пункті 5.5 цих Правил. Акредитований центр може надати таку інформацію через електронний інформаційний ресурс або в інший спосіб.

5.2.7. Договір акредитованого центру та заявника про надання послуг ЕЦП повинен включати:

обов'язки сторін, у тому числі щодо обов'язковості використання надійних засобів ЕЦП;

умови надання доступу користувачам до сертифіката підписувача (умови публікації сертифіката).

5.2.8. Договір акредитованого центру та заявника про надання послуг ЕЦП може бути у формі електронного документа.

5.2.9. Акредитований центр повинен взяти на облік укладені договори із заявниками, а також документи (посвідчені в установленому порядку копії документів), що використовуються під час реєстрації.

5.2.10. Акредитований центр повинен забезпечити захист персональних даних підписувача відповідно до законодавства.

5.3. Повторне формування сертифіката

5.3.1. При повторному формуванні сертифіката акредитований центр повинен здійснити перевірку стосовно того, що інформація, яка надавалася раніше заявником під час реєстрації, дійсна.

5.3.2. При виникненні необхідності 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 5.2 цих Правил, а час чинності особистого ключа та відповідного йому відкритого ключа не може перевищувати двох років.

5.4. Формування сертифіката

5.4.1. Формування сертифіката підписувачу здійснюється акредитованим центром на підставі даних, отриманих від заявника під час реєстрації.

5.4.2. Формат сертифіката, що відповідає вимогам Закону України "Про електронний цифровий підпис", ([852-15](#)) визначається відповідними технічними специфікаціями форматів представлення базових об'єктів національної системи ЕЦП.

5.4.3. 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.

5.4.4. Акредитований центр повинен забезпечити унікальність розпізнавального імені підписувача та реєстраційного номера сертифіката в межах акредитованого центру.

5.4.5. 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.

5.4.6. 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.

5.4.7. В акредитованому центрі повинно бути передбачено можливість резервування усіх сформованих ним сертифікатів.

5.4.8. Всі події, пов'язані із формуванням, переформуванням, блокуванням, поновленням та скасуванням сертифікатів, виданих акредитованим центром, повинні протоколюватися в акредитованому центрі із забезпеченням захисту протоколів від несанкціонованого доступу.

5.5. Розповсюдження умов обслуговування та використання сертифіката

5.5.1. 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 та 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 спорів;

законодавства в сфері ЕЦП;

підстав відповідальності акредитованого центру.

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

5.6. Розповсюдження сертифікатів

5.6.1. Після формування сертифікат повинен бути доступний заявнику та/або підписувачу, для якого цей сертифікат був сформований.

5.6.2. Доступ до сформованого сертифіката для користувачів надається у разі згоди на це заявника, якщо для державних органів інше не передбачене правилами їх систем електронного документообігу.

5.6.3. Дані, що визначені у пункті 5.5.1 та пункті 5.6.2 цих Правил, повинні бути вільно доступні для користувачів цілодобово.

5.7. Блокування та скасування сертифікатів

5.7.1. Акредитований центр повинен визначити у 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.

5.7.2. 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.

5.7.3. Підписувач, сертифікат якого був заблокований або скасований, повинен бути проінформований про зміну статусу сертифіката.

5.7.4. Скасований сертифікат не може бути в подальшому поновлений.

5.7.5. У разі, якщо для розповсюдження інформації про статус сертифіката акредитованим центром використовується механізм списку відкликаних сертифікатів, повинно бути забезпечено 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.

5.7.6. Формат списку відкликаних сертифікатів визначається відповідними технічними специфікаціями форматів представлення базових об'єктів національної системи ЕЦП.

5.7.7. Управління статусом сертифіката та розповсюдження інформації про статус сертифіката повинні бути вільнодоступні цілодобово.

5.7.8. Звернення щодо скасування сертифікатів фіксуються та зберігаються в акредитованому центрі.

5.7.9. Акредитований центр повинен забезпечити цілісність та автентичність інформації щодо статусу сертифікатів.

5.8. Час, що використовується в процесі обслуговування сертифікатів для надання послуг, повинен бути синхронізований з Всесвітнім координованим часом з точністю до однієї секунди.

6. Забезпечення безпеки інформаційних ресурсів в акредитованому центрі

6.1. Загальні вимоги

6.1.1. 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.

6.1.2. 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.

6.2. Вимоги до обслуговуючого персоналу

6.2.1. Обслуговуючий персонал акредитованого центру повинен мати відповідні знання, досвід та навички, необхідні для забезпечення надання послуг ЕЦП.

6.2.2. Функції та відповідальність обслуговуючого персоналу, діяльність якого безпосередньо пов'язана із безпекою функціонування акредитованого центру відповідно до політики безпеки акредитованого центру, повинні бути передбачені їх посадовими обов'язками (посадовими інструкціями).

6.2.3. В акредитованому центрі повинні бути визначені такі посади обслуговуючого персоналу, діяльність яких безпосередньо пов'язана із безпечним функціонуванням акредитованого центру:

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

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

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

системний адміністратор, що відповідає за функціонування програмно-технічного комплексу.

Забороняється суміщення посади адміністратора безпеки з іншими посадами.

6.3. Забезпечення безпеки фізичного середовища

6.3.1. Фізичний доступ до обладнання програмно-технічного комплексу, що забезпечує сертифікацію, управління статусом сертифіката, генерацію ключів акредитованого центру, повинен бути обмежений та надаватися тільки визначеному колу осіб із числа обслуговуючого персоналу.

6.3.2. 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 привести до виведення акредитованого центру із штатного режиму роботи.

6.3.3. Обладнання програмно-технічного комплексу, що забезпечує формування сертифіката, управління статусом сертифіката, генерацію ключів акредитованого центру, повинно розміщуватися у спеціальному приміщенні акредитованого центру, що забезпечує фізичний захист від несанкціонованого доступу до зазначених систем та даних, що ними обробляються.

6.4. Управління доступом до інформаційних ресурсів акредитованого центру

6.4.1. В акредитованому центрі повинен бути передбачений захист внутрішньої обчислювальної мережі від втручання з боку зовнішньої мережі (глобальних мереж), що є доступною для користувачів.

6.4.2. Дані про підписувача, що надаються під час реєстрації, повинні бути захищені у разі їх передавання зовнішніми комп'ютерними мережами.

6.4.3. 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).

6.4.4. Обслуговуючий персонал повинен бути успішно ідентифікований та автентифікований перед початком виконання процедур, пов'язаних із формуванням сертифіката або зміною його статусу.

6.4.5. Всі дії обслуговуючого персоналу, пов'язані із генерацією ключів формуванням сертифіката або зміною його статусу, повинні протоколюватися із забезпеченням захисту протоколів від несанкціонованого доступу.

6.4.6. Резервні копії сертифікатів та журналів аудиту програмно-технічного комплексу повинні зберігатися в окремому приміщенні із забезпеченням їх захисту від несанкціонованого доступу.

6.4.7. Програмно-технічний комплекс повинен забезпечувати реєстрацію дій обслуговуючого персоналу. Журнали аудиту системи повинні мати захист від несанкціонованого доступу, модифікації або знищення (руйнування).

6.4.8. 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 посиленних 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 у 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.

Начальник Головного управління

В.Козак

ВИМОГИ
до спеціальних приміщень
акредитованого центру

1. У цьому додатку наведені вимоги до спеціального приміщення (приміщень) акредитованого центру, які передбачають проведення заходів щодо пасивного захисту інформації від її витоку каналами побічних електромагнітних випромінювань та наведень (далі - ПЕМВН), а також від порушення її цілісності внаслідок деструктивного впливу зовнішніх електромагнітних полів.

Вимоги цього додатка повинні бути враховані при проведенні робіт зі створення КСЗІ акредитованого центру.

2. Спеціальне приміщення призначено для розташування засобів та обладнання програмно-технічного комплексу (далі - технічні засоби), за допомогою яких здійснюється генерація особистих ключів акредитованого центру та використання особистого ключа акредитованого центру, а також іншої інформації, необхідність технічного захисту якої визначена у технічному завданні на створення КСЗІ акредитованого центру.

3. Шафи (сховища тощо), що призначені для зберігання технічних засобів та виготовлені в екранованому виконанні і відповідають вимогам цього додатка, дозволяється розміщувати не в спеціальних приміщеннях акредитованого центру із забезпеченням захисту від несанкціонованого доступу до них.

4. Технічний захист інформації, у тому числі захист від впливу зовнішніх електромагнітних полів, у спеціальному приміщенні здійснюється шляхом створення умов щодо забезпечення електромагнітного екранування технічних засобів та обладнання, а також шаф відповідно до таких варіантів:

суцільне екранування усієї внутрішньої поверхні спеціального приміщення;
розміщення технічних засобів та шаф в окремії екранованій кабіні (декількох кабінах);

розміщення у неекранованому спеціальному приміщенні лише екранованих шаф і технічних засобів в екранованому виконанні;

за погодженням з контролюючим органом розміщення в неекранованому спеціальному приміщенні технічних засобів та шаф за умови забезпечення захисту інформації від витоку каналами ПЕМВН, а також порушення її цілісності внаслідок деструктивного впливу зовнішніх електромагнітних полів.

5. Для спеціальних приміщень рекомендується обирати приміщення, що відокремлені від зовнішніх стін (зі сторони оточуючої міської забудови) коридорами тощо. Розміщення спеціального приміщення під (над) санітарно-технічними кімнатами та гаражами не рекомендується.

6. Вікна спеціального приміщення повинні бути:

обладнані надійними металевими ґратами, якщо вони зовнішні та розташовані на першому чи останньому поверсі будівлі, або до яких можливе проникнення сторонніх осіб з дахів сусідніх будівель, із розташованих поруч пожежних сходів (труб водостоків тощо),

а також якщо вони є внутрішніми і мають вихід до інших приміщень акредитованого центру;

захищені від зовнішнього спостереження за допомогою скла з матовою чи рельєфною поверхнею нерівностями назовні, непрозорих штор тощо.

У разі суцільного екранування внутрішньої поверхні спеціального приміщення вікна та інші архітектурні отвори будівлі повинні бути відсутні або не повинні порушувати суцільність екрануючого покриття.

7. Спеціальне приміщення повинно бути обладнано системою контролю доступу та пожежною сигналізацією. Двері спеціального приміщення мають бути обладнані кодовим замком або системою доступу.

8. Величина ефективності екранування спеціального приміщення (або залежно від іншого варіанта пасивного захисту) та екранованих шаф для зберігання повинна складати не менше 20 дБ у діапазоні частот 0,15-1000 МГц щодо захисту від впливів зовнішніх електромагнітних полів.

9. Необхідна величина ефективності екранування та діапазон частот, у тому числі щодо рівня захищеності від витоку інформації каналами ПЕМВН, повинні визначатися на етапі проектування та облаштування спеціального приміщення залежно від достатності рівня захищеності технічних засобів від витоку інформації каналами ПЕМВН.

10. Розроблення, виготовлення, монтаж і визначення ефективності екранування спеціального приміщення повинні проводитися відповідно до вимог нормативних документів з питань технічного захисту інформації, що стосуються екранованих приміщень.

11. Спеціальне екрановане приміщення (окрема екранована кабіна (шафа), технічні засоби в екранованому виконанні) повинно оснащуватися:

протизавадними фільтрами для захисту вводів мереж електроживлення;

протизавадними фільтрами конструкції типу "поза межний хвильовід" для захисту місць вводу систем опалення, вентиляції і кондиціонування повітря;

іншими відповідними протизавадними фільтрами у разі необхідності вводів оптоволоконних мереж, сигнальних тощо.

Протизавадні фільтри за своїми характеристиками повинні забезпечувати ефективність екранування у всьому діапазоні частот екранування не нижче величин, визначених у пунктах 8 та 9 цього додатка.

12. Екрануючі поверхні спеціального приміщення (або залежно від іншого варіанта пасивного захисту) та екранованих шаф не повинні мати гальванічного зв'язку з металоконструкціями будівлі (коробами, екрануючими та захисними оболонками кабелів тощо), що мають вихід за межі контрольованої зони акредитованого центру.

13. Для електроживлення технічних засобів, що розміщуються у спеціальному приміщенні, спільно з протизавадними фільтрами захисту кіл електроживлення повинні бути встановлені пристрої безперервного електроживлення.

14. Система заземлення спеціального приміщення та її складові елементи не повинні утворювати замкнутих контурів, розміщуватися в межах контрольованої зони акредитованого центру чи у місцях із максимально ускладненим доступом до них сторонніх осіб, а також не повинні мати гальванічного зв'язку з металоконструкціями будівлі, іншими системами заземлення, екрануючими та захисними оболонками кабелів і з'єднувальних ліній, що мають вихід за межі контрольованої зони.

15. У разі необхідності об'єднання окремих технічних засобів, що розміщені у спеціальному приміщенні, у локальну обчислювальну мережу, а також введення до спеціального приміщення кабелів та ліній зв'язку необхідно здійснювати з використанням технологій волоконно-оптичних ліній зв'язку та дотриманням вимог пункту 11 цього додатка.

16. У разі, якщо за результатами спеціальних досліджень (атестації тощо) технічних засобів, розміщених у спеціальному приміщенні, виявилось недостатнім впровадження визначених у цьому додатку заходів для забезпечення захищеності інформації від витоку інформації за рахунок ПЕМВН, повинні бути впроваджені додаткові заходи з пасивного або активного захисту інформації.

Начальник Головного управління

В.Козак