



Правління Національного банку України
ПОСТАНОВА

08 вересня 20 14 року м. Київ № 553

Про затвердження Регламенту роботи
Засвідчувального центру Національного банку України

Відповідно до Закону України “Про електронний цифровий підпис”, Порядку акредитації центру сертифікації ключів, затвердженого постановою Кабінету Міністрів України від 13 липня 2004 року № 903 (зі змінами), Правил посиленої сертифікації, затверджених наказом Департаменту спеціальних телекомунікаційних систем та захисту інформації Служби безпеки України від 13 січня 2005 року № 3, зареєстрованих у Міністерстві юстиції України 27 січня 2005 року за № 104/10384 (зі змінами), з метою вдосконалення правових засад діяльності Засвідчувального центру Національного банку України Правління Національного банку України **постановляє**:

1. Затвердити Регламент роботи Засвідчувального центру Національного банку України, що додається.
2. Управлінню інформаційної безпеки (Лук'янов Д. О.) після набрання чинності цією постановою надіслати її копію до Адміністрації Державної служби спеціального зв'язку та захисту інформації України, довести її зміст до відома територіальних управлінь Національного банку України та банків України для використання в роботі.
3. Контроль за виконанням цієї постанови покласти на заступника Голови Національного банку України Смолія Я. В.
4. Постанова набирає чинності з дня її офіційного опублікування.

Голова

В. О. Гонтарева

Інд. 58

Аркуш погодження Адміністрацією Державної служби спеціального зв'язку та захисту інформації України додається.

ЗАТВЕРДЖЕНО
Постанова Правління
Національного банку України
08 вересня 2014 року № 553

Регламент роботи
Засвідчувального центру Національного банку України

I. Загальні положення

1. Цей Регламент розроблено відповідно до пунктів 7, 26 статті 7 Закону України “Про Національний банк України”, частини сьомої статті 5 та частини сьомої статті 10 Закону України “Про електронний цифровий підпис”, розпорядження Кабінету Міністрів України від 06 травня 2009 року № 483-р “Про погодження створення Засвідчувального центру Національного банку України”, Порядку акредитації центру сертифікації ключів, затвердженого постановою Кабінету Міністрів України від 13 липня 2004 року № 903 (зі змінами), Правил посиленої сертифікації, затверджених наказом Департаменту спеціальних телекомунікаційних систем та захисту інформації Служби безпеки України від 13 січня 2005 року № 3, зареєстрованих в Міністерстві юстиції України 27 січня 2005 року за № 104/10384 (у редакції наказу від 10 травня 2006 року № 50), Положення про Засвідчувальний центр Національного банку України, затвердженого постановою Правління Національного банку України від 23 вересня 2008 року № 287 (у редакції постанови Правління Національного банку України від 25 квітня 2014 року № 239), Правил реєстрації, засвідчення чинності відкритого ключа та акредитації центрів сертифікації ключів банків України в Засвідчувальному центрі Національного банку України, затверджених постановою Правління Національного банку України від 17 червня 2010 року № 284, зареєстрованих у Міністерстві юстиції України 04 листопада 2010 року за № 1035/18330 (зі змінами).

2. У цьому Регламенті терміни вживаються в такому значенні:
адміністратор безпеки Засвідчувального центру Національного банку України (далі – Засвідчувальний центр) – відповідальна особа Засвідчувального центру, яка виконує функції служби захисту інформації;

адміністратор реєстрації Засвідчувального центру – відповідальна особа Засвідчувального центру, яка виконує функції служби реєстрації;

адміністратор сертифікації Засвідчувального центру – відповідальна особа Засвідчувального центру, яка виконує функції служби сертифікації;

база даних – база даних Засвідчувального центру, у якій зберігається реєстр Засвідчувального центру, інформаційно-довідкова, технологічна та інша службова інформація, потрібна для функціонування програмно-технічного комплексу Засвідчувального центру;

ведення реєстру Засвідчувального центру – унесення (видалення, модифікація) інформації до реєстру Засвідчувального центру, її зберігання та резервування;

ключі Засвідчувального центру – власні криптографічні ключі Засвідчувального центру (особистий і відкритий) та криптографічні ключі (особистий і відкритий) послуги інтерактивного визначення статусу посиленого сертифіката відкритого ключа (далі – сертифікат ключа);

комплексна система захисту інформації Засвідчувального центру – сукупність інженерно-технічних, організаційних заходів та програмно-апаратних засобів, які забезпечують технічний та криптографічний захист інформації в програмно-технічному комплексі Засвідчувального центру;

поновлення сертифіката ключа – процедура управління статусом сертифіката ключа, що забезпечує поновлення чинності сертифіката ключа (якій передувала відповідна процедура блокування сертифіката ключа);

програмно-технічний комплекс Засвідчувального центру – сукупність технічного обладнання, програмного забезпечення та організаційних заходів, що використовується Національним банком України для забезпечення виконання функцій Засвідчувального центру;

системний адміністратор Засвідчувального центру – відповідальна особа Засвідчувального центру, що виконує функції служби системного адміністратора;

список відкликаних сертифікатів ключів Засвідчувального центру – перелік заблокованих і скасованих сертифікатів ключів, що формується Засвідчувальним центром, захист якого забезпечується накладенням електронного цифрового підпису за допомогою власних особистих ключів Засвідчувального центру;

скасування сертифіката ключа – процедура управління статусом сертифіката ключа, яка зупиняє чинність сертифіката ключа;

строк чинності сертифіката ключа – проміжок часу між датою і часом початку та датою і часом закінчення чинності сертифіката ключа, що встановлюються під час формування сертифіката ключа;

строк чинності особистого ключа – строк, протягом якого використання особистого ключа є чинним.

Інші терміни в цьому Регламенті застосовуються в значеннях, наведених у Законі України “Про електронний цифровий підпис”, Положенні про центри сертифікації ключів банків України, затвердженому постановою Правління Національного банку України від 17 червня 2010 року № 284, зареєстрованому

в Міністерстві юстиції України 04 листопада 2010 року за № 1034/18329, Правилах реєстрації, засвідчення чинності відкритого ключа та акредитації центрів сертифікації ключів банків України в Засвідчувальному центрі Національного банку України, затверджених постановою Правління Національного банку України від 17 червня 2010 року № 284, зареєстрованих у Міністерстві юстиції України 04 листопада 2010 року за № 1035/18330 (зі змінами), інших нормативно-правових актах з питань застосування електронного цифрового підпису.

3. Суб'єктами правових відносин у сфері електронного цифрового підпису, що обумовлюються цим Регламентом, є центри сертифікації ключів, які здійснюють дії, пов'язані з проведенням процедур реєстрації/акредитації в Засвідчувальному центрі, чи зареєстровані/акредитовані в Засвідчувальному центрі (далі – Центри), Засвідчувальний центр та центральний засвідчувальний орган.

4. Цей Регламент є нормативно-правовим актом, що визначає організаційно-методологічні та технологічні умови діяльності Засвідчувального центру під час проведення процедур реєстрації, засвідчення чинності відкритих ключів, акредитації Центрів у Засвідчувальному центрі, зміни ідентифікаційних даних Центрів та надання послуг електронного цифрового підпису для Центрів від Засвідчувального центру.

5. Центр зобов'язаний здійснювати свою діяльність відповідно до регламенту роботи, що визначає організаційно-методологічні та технологічні умови його діяльності в процесі надання послуг електронного цифрового підпису підписувачам. Регламент роботи Центру має розроблятися відповідно до Правил оформлення Регламенту роботи центрів сертифікації ключів банків України, затверджених постановою Правління Національного банку України від 17 червня 2010 року № 284, зареєстрованих у Міністерстві юстиції України 04 листопада 2010 року за № 1036/18331.

6. Центр зобов'язаний погодити свій регламент роботи із Засвідчувальним центром до початку проведення реєстрації/акредитації. Центр зобов'язаний додатково погодити свій регламент роботи із органом контролю до початку проведення акредитації.

7. Центр зобов'язаний кожні шість місяців надсилати електронною поштою до служби реєстрації Засвідчувального центру інформацію про діяльність Центру згідно з формою, визначеною в додатку 1 до цього Регламенту, протягом одного місяця, наступного за останнім місяцем відповідного півріччя.

8. Засвідчувальний центр має право скасувати реєстрацію/акредитацію Центру в разі ненадходження такої інформації у встановлений термін з вини Центру.

9. Адміністратор реєстрації Засвідчувального центру зобов'язаний контролювати термін вчасного подання зареєстрованим/акредитованим Центром до Засвідчувального центру інформації про діяльність Центру шляхом надсилання офіційного листа з попередженням про необхідність негайно подати звіт, якщо звіт не надійшов вчасно.

Адміністратор реєстрації Засвідчувального центру зобов'язаний проводити аналіз інформації про діяльність Центру, яка надається Центром відповідно до пункту 7 розділу I цього Регламенту, визначати потребу в перевірці виконання Центром вимог, визначених цим Регламентом та нормативно-правовими актами з питань застосування електронного цифрового підпису. Перевірка Центру проводиться, якщо кількість скарг користувачів на неправомірну діяльність (або бездіяльність) Центру протягом відповідного періоду перевищує десять. Перевірка Центру здійснюється Національним банком України в межах повноважень та згідно із законодавством України.

10. Цей Регламент установлює обов'язки Засвідчувального центру щодо використання послуг електронного цифрового підпису, які надаються центральним засвідчувальним органом, та Центрив щодо використання послуг електронного цифрового підпису, які надаються Засвідчувальним центром. Цей Регламент є засобом офіційного інформування зазначених суб'єктів у правовідносинах, що виникають під час надання та використання послуг електронного цифрового підпису.

11. Основними функціями Центру є:

- створення і забезпечення функціонування програмно-технічного комплексу Центру;
- реєстрація підписувачів;
- генерування і зберігання ключів Центру та відповідальних осіб Центру;
- забезпечення підписувачів засобами криптографічного захисту інформації (генерування ключів) і в разі потреби надання допомоги під час генерування ключів, а також ужиття заходів щодо забезпечення безпеки інформації під час їх генерування;
- засвідчення чинності відкритих ключів Центру в Засвідчувальному центрі відповідно до вимог цього Регламенту та інших нормативно-правових актів, що регулюють відносини у сфері електронного цифрового підпису;
- формування сертифікатів відкритих ключів відповідно до вимог регламенту роботи Центру та інших нормативно-правових актів, що регулюють відносини у сфері електронного цифрового підпису;
- ведення реєстру Центру;
- розповсюдження сертифікатів відкритих ключів Центру та підписувачів відповідно до вимог регламенту роботи Центру та інших нормативно-правових актів, що регулюють відносини у сфері електронного цифрового підпису;
- блокування, скасування та поновлення сертифікатів відкритих ключів, сформованих Центром, у випадках, передбачених регламентом роботи Центру і законодавством України у сфері електронного цифрового підпису;

надання підписувачам послуги фіксування часу;
 забезпечення можливості перевірки статусу сертифікатів відкритих ключів, сформованих Центром;
 публікація на інформаційному ресурсі Центру відкритої інформації;
 інші функції, визначені Законом України “Про електронний цифровий підпис”, та дії, пов’язані з технічною і технологічною підтримкою діяльності Центру.

12. Ідентифікаційні дані Засвідчувального центру:

Повне найменування: Засвідчувальний центр Національного банку України.

Місцезнаходження: 01601, м. Київ, вул. Інститутська, 9.

Адреси розміщення Засвідчувального центру:

03028, м. Київ, просп. Науки, 7;

01601, м. Київ, вул. Інститутська, 9.

Телефон: (044) 525-37-36.

Факс: (044) 524-39-63.

Код за ЄДРПОУ: 00032106.

Електронна адреса інформаційного ресурсу (веб-сайта):
<http://zc.bank.gov.ua>.

II. Організаційна структура Засвідчувального центру

1. Організаційна структура Засвідчувального центру містить дві основні складові, що виконують адміністративні, технічні й технологічні функції.

2. Адміністративні функції Засвідчувального центру:

реєстрація Центрив;

акредитація Центрив;

видача, переоформлення та анулювання свідоцтв/дублікатів свідоцтв про реєстрацію/акредитацію Центрив;

забезпечення діяльності Комісії з питань реєстрації, акредитації, повторної акредитації, скасування реєстрації та акредитації, погодження регламентів роботи Центрив;

ведення списку Центрив, що припинили діяльність;

надання Центрам консультацій з питань, пов’язаних із використанням електронного цифрового підпису;

погодження регламентів роботи Центрив;

аналіз інформації про діяльність Центрив, розгляд заяв і скарг щодо неналежного функціонування Центрив та вживання відповідних заходів;

приймання на зберігання від Центрив документованої інформації, яка підлягає передаванню в разі скасування реєстрації, акредитації чи припинення їх діяльності.

3. Технічні й технологічні функції Засвідчувального центру:

створення і забезпечення функціонування програмно-технічного комплексу Засвідчувального центру;

забезпечення захисту інформації впродовж експлуатації програмно-технічного комплексу Засвідчувального центру;

генерування і зберігання ключів Засвідчувального центру та відповідальних осіб Засвідчувального центру;

вивантаження з програмно-технічного комплексу Засвідчувального центру власних відкритих ключів Засвідчувального центру для засвідчення їх чинності в центральному засвідчувальному органі;

установлення належності Центру особистого ключа та його відповідності відкритому ключу під час формування сертифіката ключа Центру;

формування сертифікатів ключів відповідно до вимог цього Регламенту та інших нормативно-правових актів, що регулюють відносини у сфері електронного цифрового підпису;

ведення реєстру Засвідчувального центру;

поширення сертифікатів ключів Засвідчувального центру та Центрів у встановленому цим Регламентом порядку;

блокування, скасування та поновлення сертифікатів ключів, сформованих Засвідчувальним центром, у випадках, передбачених цим Регламентом і законодавством України у сфері електронного цифрового підпису;

забезпечення можливості визначення статусу сертифікатів ключів, сформованих Засвідчувальним центром;

оприлюднення на інформаційному ресурсі Засвідчувального центру відкритої інформації;

інші дії, пов'язані з технічною й технологічною підтримкою діяльності Засвідчувального центру.

4. У Засвідчувальному центрі для виконання адміністративних, технічних і технологічних функцій створено такі служби:

- служба захисту інформації;
- служба сертифікації;
- служба реєстрації;
- служба системного адміністратора.

5. Основними функціями служби захисту інформації є:

- проекування, розроблення, експлуатація, обслуговування та модернізація комплексної системи захисту інформації Засвідчувального центру;
- адміністрування відповідальних осіб Засвідчувального центру.

6. Основними функціями служби сертифікації є:
- генерування ключів Засвідчувального центру;
 - збереження та використання особистих ключів Засвідчувального центру;
 - збереження та використання особистих ключів Засвідчувального центру;

вивантаження з апаратури криптографічних засобів захисту інформації (далі – АКЗЗІ) власних відкритих ключів Засвідчувального центру для засвідчення їх чинності в центральному засвідчувальному органі;

завантаження сертифікатів власних ключів Засвідчувального центру в програмно-технічний комплекс Засвідчувального центру;

перехід на використання нових ключів Засвідчувального центру;

знищення особистих ключів Засвідчувального центру, строк чинності яких закінчився;

засвідчення чинності відкритих ключів Центрів та послуги інтерактивного визначення статусу сертифіката ключа;

звернення до центрального засвідчувального органу щодо зміни статусу сертифікатів власних ключів Засвідчувального центру у випадках, передбачених цим Регламентом і законодавством України у сфері електронного цифрового підпису;

управління статусом сертифікатів ключів, сформованих Засвідчувальним центром;

унесення змін до реєстру Засвідчувального центру щодо статусу Центру (Центр може мати один із таких статусів: збережений, зареєстрований, акредитований, анульований);

забезпечення можливості визначення статусу сертифікатів ключів, сформованих Засвідчувальним центром;

вивантаження/завантаження резервної інформації із/в програмно-технічний комплекс Засвідчувального центру.

7. Основними функціями служби реєстрації є:

установлення осіб заявників Центрів;

перевірка Центрів у процесі їх реєстрації, акредитації та подальшої роботи на відповідність вимогам, установленим цим Регламентом та іншими нормативно-правовими актами у сфері електронного цифрового підпису;

опрацювання документів і запитів, які подаються заявником Центру до Засвідчувального центру під час проведення регламентних процедур;

уведення в програмно-технічний комплекс Засвідчувального центру запитів на формування сертифікатів ключів Центрів для засвідчення їх чинності;

формування в програмно-технічному комплексі Засвідчувального центру запитів на блокування, поновлення та скасування сертифікатів ключів Центрів у разі подання відповідних заяв (додаток 2);

контроль за строками подання акредитованими Центрами до Засвідчувального центру інформації про діяльність Центрів за формою, установленною в додатку 1 до цього Регламенту, та її опрацювання.

8. Основними функціями служби системного адміністратора є:

установлення та налаштування операційної системи на робочих місцях відповідальних осіб Засвідчувального центру та на серверах Засвідчувального центру;

установлення та налаштування серверних і клієнтських застосувань на робочих місцях відповідальних осіб Засвідчувального центру та на серверах Засвідчувального центру;

виконання оновлень серверного та клієнтського програмного забезпечення програмно-технічного комплексу Засвідчувального центру;

під'єднання робочих місць відповідальних осіб Засвідчувального центру та серверів Засвідчувального центру до інформаційної мережі Національного банку України;

підтримка належного функціонування програмно-технічного комплексу Засвідчувального центру.

9. У Засвідчувальному центрі для виконання завдань, покладених на зазначені в пункті 4 цього розділу служби, створено такі автоматизовані робочі місця:

автоматизовані робочі місця адміністраторів безпеки Засвідчувального центру;

автоматизовані робочі місця адміністраторів сертифікації Засвідчувального центру;

автоматизовані робочі місця адміністраторів реєстрації Засвідчувального центру;

неспеціалізовані автоматизовані робочі місця.

10. Відповідальні особи Засвідчувального центру виконують функції служб, зазначених у пункті 4 цього розділу, на відповідних спеціалізованих автоматизованих робочих місцях.

11. Відповідальні особи Засвідчувального центру мають право виконувати роботу з нормативно-довідковою інформацією Засвідчувального центру на своїх спеціалізованих автоматизованих робочих місцях або на неспеціалізованому автоматизованому робочому місці з дотриманням вимог, визначених політикою безпеки інформації в програмно-технічному комплексі Засвідчувального центру, у межах повноважень, наданих їм адміністратором безпеки Засвідчувального центру.

12. Відповідальна особа Засвідчувального центру не має права суміщувати функції служби захисту інформації Засвідчувального центру з функціями інших служб у Засвідчувальному центрі.

13. Усі відповідальні особи Засвідчувального центру перед початком виконання своїх функціональних обов'язків зобов'язані ознайомитися зі змістом цього Регламенту, інструкцій щодо роботи на автоматизованих робочих місцях, інструкції щодо забезпечення безпеки експлуатації засобів криптографічного захисту інформації та порядку генерування ключових даних і поводження з ключовими документами (далі – інструкції щодо роботи з

ключовими даними). Відповідальні особи Засвідчувального центру підтверджують факт ознайомлення з цими документами під підпис.

III. Архітектура програмно-технічного комплексу Засвідчувального центру

1. Графічна архітектура та загальна технологічна схема оброблення інформації в програмно-технічному комплексі Засвідчувального центру зображені на рис. 1.

2. Програмно-технічний комплекс Засвідчувального центру є автоматизованою системою класу 3. Технічні засоби комплексу об'єднані в розподілену обчислювальну мережу з використанням інформаційної мережі Національного банку України, частина з яких підключена до зовнішніх телекомунікаційних мереж.

3. Апаратне комп'ютерне забезпечення програмно-технічного комплексу Засвідчувального центру складається з двох типів комп'ютерної техніки, а саме:

- серверної комп'ютерної техніки;
- клієнтської комп'ютерної техніки.

4. Програмне забезпечення програмно-технічного комплексу Засвідчувального центру є централізованим трирівневим комплексом, що складається з таких компонентів:

- база даних;
- серверні застосування;
- клієнтські застосування.

5. База даних, клієнтське застосування системи керування базою даних та серверні застосування функціонують у серверній комп'ютерній техніці.

6. Усі інші клієнтські застосування, що використовуються в програмно-технічному комплексі Засвідчувального центру, функціонують у клієнтській комп'ютерній техніці, яка входить до складу автоматизованих робочих місць відповідальних осіб Засвідчувального центру.

7. У програмно-технічному комплексі Засвідчувального центру організовано основні та резервні автоматизовані робочі місця адміністратора сертифікації Засвідчувального центру та адміністратора безпеки Засвідчувального центру. Забороняється одночасно експлуатувати основне та резервне автоматизовані робочі місця адміністратора сертифікації Засвідчувального центру. Забороняється одночасно експлуатувати основне та резервне автоматизовані робочі місця адміністратора безпеки Засвідчувального центру.

клієнтські робочі місця ПТК Засвідчувального центру

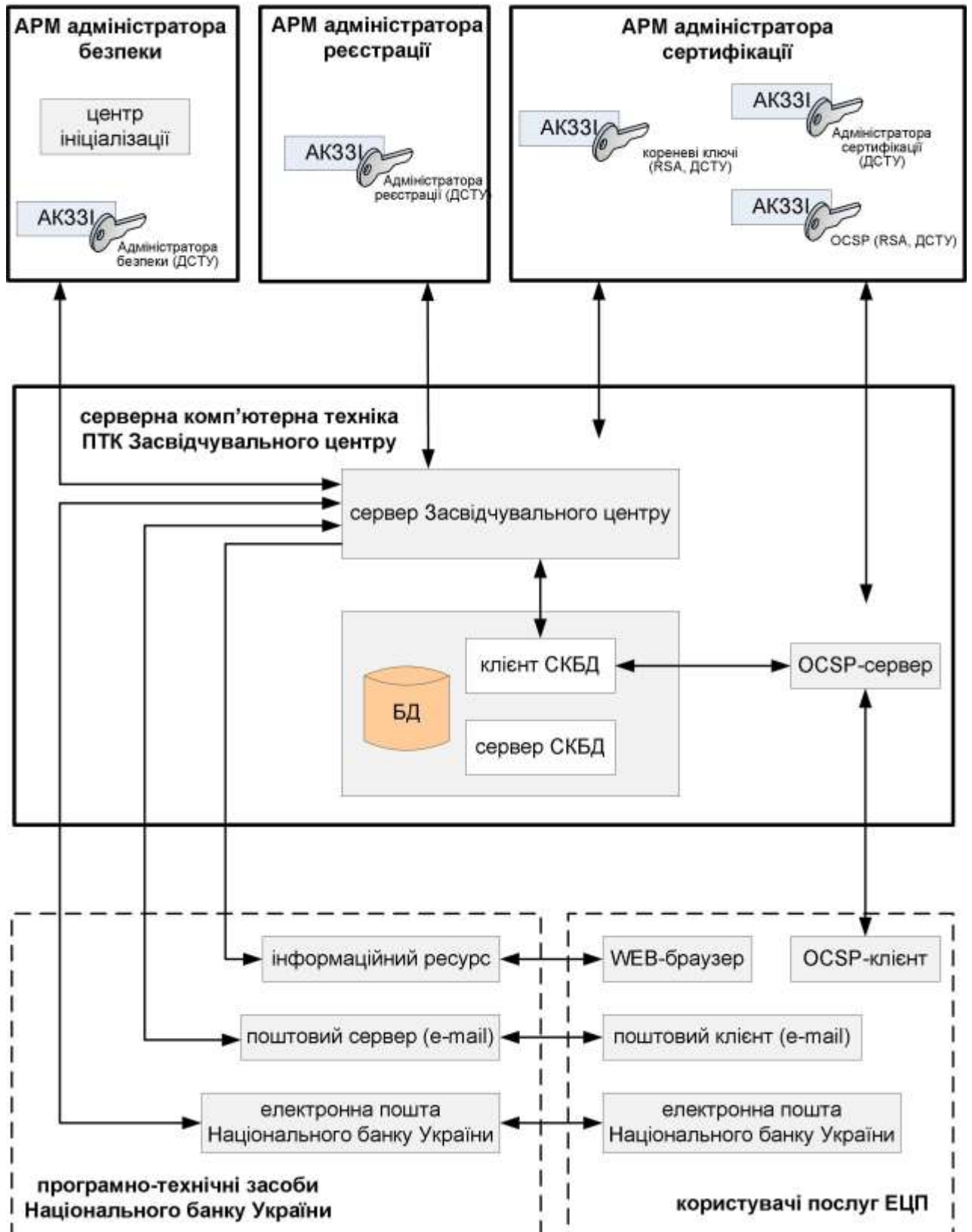


рис. 1. Архітектура програмно-технічного комплексу Засвідчувального центру

8. Сервер Засвідчувального центру виконує такі технічні й технологічні функції програмно-технічного комплексу Засвідчувального центру:

ініціювання завантаження/вивантаження інформації до/із бази даних шляхом використання клієнтського застосування системи керування базою даних (за запитом клієнтських застосувань, установлених на автоматизованих робочих місцях відповідальних Засвідчувального центру, та під час поширення сертифікатів ключів і списку відкликаних сертифікатів ключів Засвідчувального центру);

формування сертифікатів ключів;

створення запитів на блокування, скасування та поновлення сертифікатів ключів;

блокування, скасування та поновлення сертифікатів ключів;

формування списку відкликаних сертифікатів ключів Засвідчувального центру;

поширення сертифікатів ключів;

поширення списку відкликаних сертифікатів ключів Засвідчувального центру;

зберігання нормативно-довідкової інформації Засвідчувального центру;

ідентифікація, автентифікація та авторизація відповідальних осіб Засвідчувального центру;

ведення журналів аудиту функціонування сервера Засвідчувального центру.

9. Сервер надання послуги інтерактивного визначення статусу сертифіката ключа (сервер OCSP) надає послугу інтерактивного визначення статусу сертифіката ключа, сформованого Засвідчувальним центром.

10. Сервер системи керування базою даних виконує такі технічні й технологічні функції програмно-технічного комплексу Засвідчувального центру:

управління даними бази даних (завантаження/вивантаження інформації до/із бази даних, створення нових записів тощо);

ведення журналів аудиту функціонування бази даних;

резервне копіювання бази даних;

відновлення бази даних після збоїв.

11. За допомогою клієнтських застосувань ініціюється:

виконання технічних і технологічних функцій програмно-технічного комплексу Засвідчувального центру з використанням серверних застосувань;

генерування і зберігання криптографічних ключів Засвідчувального центру та відповідальних осіб Засвідчувального центру засобами АКЗЗІ;

вивантаження з АКЗЗІ відкритих ключів Засвідчувального центру для засвідчення їх чинності відповідно до вимог цього Регламенту та інших нормативно-правових актів, що регулюють відносини у сфері електронного цифрового підпису.

12. Лише за допомогою серверних застосувань може проводитися завантаження/вивантаження інформації до/із бази даних шляхом використання клієнтського застосування системи керування бази даних. Клієнтські застосування, що функціонують у складі автоматизованих робочих місць, отримують доступ до інформації в базі даних за допомогою серверних застосувань.

13. Серверні застосування програмно-технічного комплексу Засвідчувального центру функціонують на базі відмовостійкого кластера.

14. Моніторинг роботи кластера здійснює Єдина система моніторингу та управління інформаційними ресурсами Національного банку України.

IV. Режими доступу до інформації у Засвідчувальному центрі

1. У Засвідчувальному центрі приймається, обробляється, пересилається і зберігається інформація, яка за режимом доступу поділяється на відкриту інформацію та інформацію з обмеженим доступом, що має гриф “банківська таємниця” та “конфіденційно”.

2. Відкрита інформація може оприлюднюватися шляхом її розміщення на інформаційному ресурсі Засвідчувального центру і розсилання засобами електронної пошти (e-mail) та електронної пошти Національного банку України.

3. Доступ до інформації з обмеженим доступом Засвідчувального центру мають керівник/заступник керівника та відповідальні особи Засвідчувального центру з дотриманням вимог, визначених політикою безпеки інформації в Засвідчувальному центрі.

4. Засвідчувальний центр має право надавати доступ до інформації з обмеженим доступом іншим особам лише у випадках, передбачених законодавством України.

5. До відкритої інформації Засвідчувального центру належать:
положення цього Регламенту;
нормативні документи та довідкові матеріали;
зразок договору про надання Засвідчувальним центром послуг Центру (далі – договір про надання послуг);
примірний регламент роботи Центру;
сертифікати ключів Засвідчувального центру та Центрів;
інформація про статус сертифікатів ключів Засвідчувального центру та Центрів;

частина бази даних, у якій міститься інформація про Центри, що вноситься в сертифікати ключів Центрів та оприлюднюється шляхом розміщення на інформаційному ресурсі Засвідчувального центру.

Відкрита інформація може зберігатися на паперових носіях та в електронній формі.

6. До відкритої інформації, яка потребує захисту (забезпечення цілісності та доступності), належить інформація, що оприлюднюється шляхом розміщення на інформаційному ресурсі Засвідчувального центру.

7. До інформації з обмеженим доступом Засвідчувального центру в електронній формі належать:

особисті ключі Засвідчувального центру та відповідальних осіб Засвідчувального центру;

частина бази даних, у якій міститься інформація про Центри, що не підлягає безпосередньому оприлюдненню (персональні дані про заявника, керівника та заступників керівників Центрів, списки відповідальних осіб Центрів, плани-схеми приміщень Центрів, порядок доступу до спеціальних приміщень та інша інформація, яка не оприлюднюється на електронному інформаційному ресурсі Засвідчувального центру);

налаштування програмних засобів програмно-технічного комплексу Засвідчувального центру (налаштування комплексу засобів захисту, перелік мережевих адрес, протоколів і портів, що використовуються для забезпечення взаємодії між клієнтськими та серверними застосуваннями тощо);

списки відповідальних осіб Засвідчувального центру, їх ідентифікаторів, повноважень, права доступу, зміст протоколів роботи програмно-технічного комплексу Засвідчувального центру тощо;

журнали аудиту, які ведуться в електронній формі.

8. До інформації з обмеженим доступом Засвідчувального центру на паперових носіях належать:

документи, що подаються Центрами до Засвідчувального центру під час проведення регламентних процедур і не підлягають безпосередньому оприлюдненню;

журнали аудиту, які ведуться на паперових носіях;

інструкції відповідальних осіб Засвідчувального центру;

інструкції щодо роботи з ключовими даними.

V. Захист інформації в Засвідчувальному центрі

1. Захист інформації в Засвідчувальному центрі забезпечується в результаті впровадження комплексної системи захисту інформації. Комплексна система захисту інформації повинна мати атестат відповідності вимогам захисту інформації.

2. Усі складові частини програмно-технічного комплексу Засвідчувального центру перебувають у межах контрольованих зон Центрального апарату, Центральної розрахункової палати чи територіального управління Національного банку України (залежить від місця розташування конкретної частини програмно-технічного комплексу Засвідчувального центру).

3. Серверна комп'ютерна техніка програмно-технічного комплексу Засвідчувального центру розміщується в спеціальних серверних приміщеннях (у будівлях Національного банку України за адресами: м. Київ, вул. Інститутська, 9; м. Київ, просп. Науки, 7), що відповідають вимогам Правил з технічного захисту інформації для приміщень банків, у яких обробляються електронні банківські документи, затверджених постановою Правління Національного банку України від 04 липня 2007 року № 243, та додатка до Правил посиленої сертифікації, затверджених наказом Департаменту спеціальних телекомунікаційних систем та захисту інформації Служби безпеки України від 13 січня 2005 року № 3, зареєстрованих у Міністерстві юстиції України 27 січня 2005 року за № 104/10384 (у редакції наказу від 10 травня 2006 року № 50).

4. Основне та резервне автоматизовані робочі місця адміністратора сертифікації Засвідчувального центру розміщуються в будівлях Національного банку України за адресами: м. Київ, просп. Науки, 7; м. Київ, вул. Інститутська, 9. Обидва автоматизовані робочі місця розміщені в екранованих шафах, які розташовані в спеціальних приміщеннях з обмеженим доступом. Ключі від екранованих шаф мають тільки адміністратори сертифікації Засвідчувального центру. Спеціальні приміщення та екрановані шафи відповідають вимогам Правил з технічного захисту інформації для приміщень банків, у яких обробляються електронні банківські документи, затверджених постановою Правління Національного банку України від 04 липня 2007 року № 243, та додатка до Правил посиленої сертифікації, затверджених наказом Департаменту спеціальних телекомунікаційних систем та захисту інформації Служби безпеки України від 13 січня 2005 року № 3, зареєстрованих у Міністерстві юстиції України 27 січня 2005 року за № 104/10384 (у редакції наказу від 10 травня 2006 року № 50). Адміністратор безпеки Засвідчувального центру отримує доступ до автоматизованого робочого місця адміністратора сертифікації Засвідчувального центру тільки на час проведення процедури генерування криптографічних ключів Засвідчувального центру.

5. Клієнтська комп'ютерна техніка інших відповідальних осіб Засвідчувального центру розміщується в тих самих приміщеннях, у яких працюють ці відповідальні особи Засвідчувального центру.

6. Сторонні особи не мають доступу до приміщень, у яких розташовано обладнання програмно-технічного комплексу Засвідчувального центру. Ці приміщення перебувають під цілодобовою охороною, оснащені охоронною сигналізацією, датчиками руху та датчиками пожежної сигналізації. Ключі від приміщень видаються охороною тільки авторизованому персоналу. Такі умови розміщення обладнання програмно-технічного комплексу Засвідчувального центру забезпечують захищеність середовища його розміщення та унеможливають несанкціоноване проникнення до програмно-технічного комплексу Засвідчувального центру.

7. Усі засоби криптографічного захисту інформації програмно-технічного комплексу Засвідчувального центру повинні мати позитивний експертний висновок за результатами державної експертизи у сфері криптографічного захисту інформації.

8. Усі особисті ключі, що використовуються в Засвідчувальному центрі, зберігаються виключно всередині пристроїв АКЗЗІ. Відкриті ключі відповідальних осіб Засвідчувального центру зберігаються виключно всередині АКЗЗІ та в базі даних програмно-технічного комплексу Засвідчувального центру. Сертифікати ключів, сформовані Засвідчувальним центром, розповсюджуються в порядку, установленому цим Регламентом.

9. Відповідальні особи Засвідчувального центру зобов'язані здійснювати генерування і використання криптографічних ключів відповідно до своїх функціональних обов'язків виключно засобами АКЗЗІ на своїх спеціалізованих автоматизованих робочих місцях.

10. Відповідальні особи Засвідчувального центру зобов'язані зберігати інформацію з обмеженим доступом на паперових носіях чи в електронному вигляді на зйомних носіях (у тому числі в АКЗЗІ), у сейфах/ящиках/шафах, що надійно замикаються і до яких не мають доступу сторонні особи.

11. Відповідальні особи Засвідчувального центру несуть особисту відповідальність за надійне зберігання АКЗЗІ та нерозголошення значення паролів доступу і розблокування.

12. Адміністратор безпеки Засвідчувального центру та адміністратор сертифікації Засвідчувального центру зобов'язані зберігати свої основні пристрої АКЗЗІ на своїх основних робочих місцях, а резервні пристрої АКЗЗІ – на резервних робочих місцях.

13. Адміністратор сертифікації Засвідчувального центру зобов'язаний зберігати основні та частину резервних АКЗЗІ з ключами Засвідчувального центру в екранованій шафі на основному робочому місці, а іншу частину резервних АКЗЗІ – в екранованій шафі на резервному робочому місці.

Адміністратор сертифікації Засвідчувального центру несе особисту відповідальність за надійне зберігання цих АКЗЗІ та нерозголошення паролів доступу і розблокування.

14. Адміністратор сертифікації Засвідчувального центру зобов'язаний забезпечити зберігання резервних копій бази даних Засвідчувального центру на зйомних носіях в екранованих шафах на своїх основному та резервному робочих місцях.

15. Серверні застосування та всі автоматизовані робочі місця забезпечують можливість:

криптографічного захисту інформації, що передається каналами зв'язку (автентифікація та шифрування);

захищеного від модифікації протоколювання подій, визначених цим Регламентом;

використання засобів антивірусного захисту на комп'ютерах програмно-технічного комплексу Засвідчувального центру.

16. Захист інформації, що надається заявником Центру для проведення регламентних процедур (у тому числі персональних даних керівника Центру, заступників керівників Центру та заявника Центру), забезпечується шляхом ужиття:

організаційних заходів щодо обліку та зберігання справ Центрів (формування справ Центрів та їх облік; призначення осіб, відповідальних за зберігання справ Центрів; обмеження доступу до приміщень (шаф), у яких зберігаються справи Центрів);

організаційно-технічних і технічних заходів, реалізованих у результаті впровадження комплексної системи захисту інформації, у тому числі використання надійних засобів електронного цифрового підпису, ведення журналів роботи програмно-технічного комплексу Засвідчувального центру в захищеному вигляді, розмежування та здійснення контролю за інформаційними потоками між внутрішньою локальною мережею Засвідчувального центру і підсистемою відкритого доступу, використання антивірусних засобів, міжмережєвих екранів тощо.

VI. Журнали аудиту в програмно-технічному комплексі Засвідчувального центру

1. У програмно-технічному комплексі Засвідчувального центру ведуться такі журнали аудиту:

функціонування програмного забезпечення та АКЗЗІ в програмно-технічному комплексі Засвідчувального центру;

обліку АКЗЗІ;

обліку носіїв інформації з резервними копіями бази даних Засвідчувального центру;

проведення регламентних процедур;
технічного обслуговування програмно-технічного комплексу
Засвідчувального центру.

2. Журнали функціонування програмного забезпечення та АКЗЗІ в програмно-технічному комплексі Засвідчувального центру ведуться в електронній формі на всіх серверних та клієнтських застосуваннях. Інші журнали ведуться в електронній формі або на паперових носіях. Журнали аудиту, які ведуться в електронній формі, повинні мати захист від модифікації.

3. Програмне забезпечення програмно-технічного комплексу Засвідчувального центру забезпечує захищене від модифікації протоколювання подій, пов'язаних з функціонуванням програмного забезпечення та АКЗЗІ. Цей журнал подій містить дату та час події, опис події, а також ідентифікатор суб'єкта, що ініціював цю подію. У журналі реєструються події, пов'язані з:

генеруванням, резервуванням, використанням і знищенням особистих ключів Засвідчувального центру та відповідальних осіб Засвідчувального центру;

формуванням, переформуванням, блокуванням, поновленням та скасуванням сертифікатів ключів;

унесенням, модифікацією та вилученням даних про Засвідчувальний центр, відповідальних осіб Засвідчувального центру (у тому числі інформації про їх права доступу до програмно-технічного комплексу Засвідчувального центру) та Центри;

наданням доступу до програмно-технічного комплексу Засвідчувального центру відповідальним особам Засвідчувального центру, у тому числі зі спробами несанкціонованого доступу до програмно-технічного комплексу Засвідчувального центру;

збоями в роботі програмно-технічного комплексу Засвідчувального центру;

установленням, зміною, знищенням паролів та системних привілеїв відповідальних осіб Засвідчувального центру.

4. Адміністратор безпеки Засвідчувального центру зобов'язаний вести журнал подій, пов'язаних з обліком АКЗЗІ, яка використовується в Засвідчувальному центрі. Цей журнал подій містить дату та час події, опис події, серійний номер АКЗЗІ, підпис адміністратора безпеки Засвідчувального центру. У журналі реєструються події, пов'язані з видачею/поверненням АКЗЗІ відповідальними особами Засвідчувального центру.

5. Адміністратор сертифікації Засвідчувального центру зобов'язаний вести журнал подій, пов'язаних з обліком носіїв інформації, на яких зберігається резервна копія бази даних Засвідчувального центру. Цей журнал подій містить дату і час події, опис події, назву та серійний номер носія, підпис адміністратора сертифікації Засвідчувального центру.

6. Адміністратор реєстрації Засвідчувального центру зобов'язаний вести журнал подій, пов'язаних з проведенням регламентних процедур. Цей журнал подій містить дату події, опис події, реєстраційний номер поданої заяви, реєстраційний номер рішення про виконання чи відмову від здійснення відповідної регламентної процедури, підпис адміністратора реєстрації Засвідчувального центру. У журналі реєструються події, пов'язані з:

прийманням заяв про реєстрацію Центру в Засвідчувальному центрі (додаток 3), про акредитацію Центру в Засвідчувальному центрі (додаток 4), про формування посиленого сертифіката відкритого ключа Центру в Засвідчувальному центрі (додаток 5), про зміну статусу сертифіката ключа Центру, про внесення змін до реєстраційних даних зареєстрованого/акредитованого Центру в Засвідчувальному центрі (додаток 6), про видачу дублікату свідоцтва про реєстрацію/акредитацію Центру в Засвідчувальному центрі (додаток 7);

прийняттям рішення про виконання чи відмову в проведенні реєстрації/акредитації/формуванні сертифікатів ключів;

унесенням даних Центру до реєстру Засвідчувального центру;

видачею/скасуванням свідоцтв про реєстрацію/акредитацію Центру в Засвідчувальному центрі (додаток 8) та дублікатів цих свідоцтв.

7. Системний адміністратор зобов'язаний вести журнал регламентних робіт із технічного обслуговування програмно-технічного комплексу Засвідчувального центру. Цей журнал подій містить дату та час події, опис події. У журналі реєструються події, пов'язані з:

плановою заміною комп'ютерної техніки програмно-технічного комплексу Засвідчувального центру;

виходом з ладу складових частин комп'ютерної техніки програмно-технічного комплексу Засвідчувального центру та їх ремонтом/заміною;

оновленням програмного забезпечення Засвідчувального центру.

8. Відповідальні особи Засвідчувального центру, які ведуть журнали аудиту на паперових носіях або в електронній формі на зйомних носіях, зобов'язані зберігати їх у сейфах/ящиках/шафах, що надійно замикаються і до яких не мають доступу сторонні особи.

9. Відповідальні особи Засвідчувального центру зобов'язані здійснювати резервне копіювання журналів аудиту. Відповідальні особи Засвідчувального центру здійснюють резервне копіювання журналів аудиту в електронній формі шляхом їх запису на зйомні носії. Відповідальні особи Засвідчувального центру здійснюють резервне копіювання журналів аудиту на паперових носіях шляхом сканування та запису на зйомні носії.

10. Відповідальні особи Засвідчувального центру зобов'язані забезпечити зберігання резервних копій журналів аудиту в приміщеннях, що територіально

відокремлені від приміщень Засвідчувального центру, із забезпеченням їх захисту від несанкціонованого доступу.

11. Відповідальні особи Засвідчувального центру мають право переглядати журнали аудиту в програмно-технічному комплексі Засвідчувального центру в разі потреби.

12. Відповідальні особи Засвідчувального центру (крім адміністратора безпеки Засвідчувального центру) зобов'язані отримати дозвіл від керівника/заступника керівника Засвідчувального центру на перегляд журналів аудиту, що ведуться:

з використанням серверних застосувань (крім системних адміністраторів, які відповідають за функціонування операційної системи чи прикладного програмного забезпечення на серверній комп'ютерній техніці);

з використанням клієнтських застосувань на інших автоматизованих робочих місцях;

іншими відповідальними особами Засвідчувального центру.

13. Строк зберігання резервних копій журналів аудиту в програмно-технічному комплексі Засвідчувального центру становить п'ять років з дати здійснення резервного копіювання.

VII. Особисті та відкриті ключі

1. У Засвідчувальному центрі генеруються та використовуються такі криптографічні ключі:

власні (особистий та відкритий) ключі Засвідчувального центру для криптографічного алгоритму за ДСТУ 4145 – 2002 (довжина не менше 257 біт);

власні (особистий та відкритий) ключі Засвідчувального центру для криптографічного алгоритму RSA (довжина не менше 2048 біт);

особистий та відкритий ключі послуги інтерактивного визначення статусу сертифіката ключа для криптографічного алгоритму за ДСТУ 4145 – 2002 (довжина не менше 257 біт);

особистий та відкритий ключі послуги інтерактивного визначення статусу сертифіката ключа для криптографічного алгоритму RSA (довжина не менше 2048 біт);

особисті та відкриті ключі відповідальних осіб Засвідчувального центру для криптографічного алгоритму за ДСТУ 4145 – 2002 (довжина не менше 191 біта).

2. Власні особисті ключі Засвідчувального центру використовуються для формування сертифікатів ключів Центрів, Засвідчувального центру (крім сертифікатів власних ключів Засвідчувального центру для криптографічного алгоритму за ДСТУ 4145 – 2002) та списків відкликаних сертифікатів ключів Засвідчувального центру.

3. Особисті ключі послуги інтерактивного визначення статусу сертифіката ключа використовуються під час формування відповіді на запит про визначення статусу сертифіката ключа.

4. Особисті ключі відповідальних осіб Засвідчувального центру використовуються виключно для їх автентифікації, авторизації, забезпечення цілісності інформації та спостережності в програмно-технічному комплексі Засвідчувального центру.

5. Центр самостійно генерує особисті та відкриті ключі Центру. Засвідчувальний центр не надає послуг з генерації ключів для Центру.

6. Довжина особистих ключів для зареєстрованого Центру або Центру, що проходить реєстрацію, має бути:

для алгоритму ДСТУ 4145-2002 – не менше 162 біт;

для алгоритму RSA – не менше 1 536 біт.

7. Довжина особистих ключів для акредитованого Центру або Центру, що проходить акредитацію, має бути:

для алгоритму ДСТУ 4145-2002 – не менше 257 біт;

для алгоритму RSA – не менше 2 048 біт.

8. Центр зобов'язаний:

використовувати особисті ключі Центру для формування списку відкликаних сертифікатів ключів Центру та сертифікатів ключів підписувачів, які є клієнтами цього Центру;

використовувати та зберігати особистий ключ та фразу-пароль для голосової автентифікації у спосіб, що унеможливорює ознайомлення з ними сторонніх осіб;

звернутися до служби реєстрації Засвідчувального центру щодо блокування/скасування сертифіката ключа внаслідок виявлення даних про: утрату або компрометацію особистого ключа Центру; утрату контролю за особистим ключем Центру через компрометацію пароля (коду, персонального ідентифікаційного номера), доступу до нього; зміну відомостей, зазначених у сертифікаті ключа Центру;

негайно припинити використання особистого ключа Центру після подання заяви про блокування/скасування відповідного йому сертифіката ключа Центру;

не використовувати особистий ключ Центру в разі його компрометації чи втрати чинності відповідного йому сертифіката ключа Центру.

9. Центр має право використовувати особисті ключі Центру для формування сертифікатів ключів відповідальних осіб Центру та послуги інтерактивного визначення статусу сертифіката ключа.

10. Відкритий ключ відповідальної особи Засвідчувального центру використовується виключно для її ідентифікації, автентифікації та авторизації під час завантаження автоматизованого робочого місця та перевірки електронного цифрового підпису, що накладається нею на документи під час виконання своїх функціональних обов'язків.

11. Строк чинності особистого та відкритого ключів дорівнює строку чинності відповідного сертифіката ключа. Особистий ключ тимчасово не є чинним, якщо сертифікат відповідного йому відкритого ключа заблоковано.

12. Строк чинності особистого та відкритого ключів відповідальної особи Засвідчувального центру становить не більше двох років з дати і часу їх генерування.

13. Адміністратор сертифікації Засвідчувального центру зобов'язаний здійснювати процедури генерування та резервування ключів Засвідчувального центру на своєму автоматизованому робочому місці. Процедури здійснюються під контролем адміністратора безпеки Засвідчувального центру. Резервування здійснюється на кількох пристроях АКЗЗІ. Резервування можна провести тільки під час генерування ключів Засвідчувального центру.

14. Адміністратор сертифікації Засвідчувального центру зобов'язаний використовувати резервні копії особистих ключів Засвідчувального центру в разі:

виходу з ладу основних пристроїв АКЗЗІ з ключами Засвідчувального центру;

експлуатації резервного автоматизованого робочого місця адміністратора сертифікації Засвідчувального центру.

15. Відповідальні особи Засвідчувального центру зобов'язані виконувати генерування ключів, які використовуватимуться для виконання їх функціональних обов'язків, на своїх спеціалізованих автоматизованих робочих місцях.

16. Адміністратор сертифікації Засвідчувального центру зобов'язаний приймати рішення про факт або загрозу компрометації особистих ключів Засвідчувального центру чи паролів доступу до пристроїв АКЗЗІ, на яких вони записані.

17. Адміністратор сертифікації Засвідчувального центру в разі компрометації або підозри на компрометацію будь-якого з особистих ключів Засвідчувального центру зобов'язаний забезпечити скасування або блокування відповідного сертифіката ключа Засвідчувального центру в спосіб, визначений цим Регламентом.

18. Відповідальна особа Засвідчувального центру зобов'язана приймати рішення про факт або загрозу компрометації свого особистого ключа чи пароля доступу до АКЗЗІ.

19. Відповідальна особа Засвідчувального центру зобов'язана ініціювати блокування свого облікового запису та формування нових криптографічних ключів в установленому цим Регламентом порядку в разі компрометації чи підозри на компрометацію особистого ключа.

20. Відповідальна особа Засвідчувального центру зобов'язана припинити роботу в програмно-технічному комплексі Засвідчувального центру та змінити пароль доступу до АКЗЗІ в разі компрометації чи підозри на компрометацію пароля доступу.

21. Адміністратор сертифікації Засвідчувального центру зобов'язаний знищити основні та всі резервні копії особистих ключів Засвідчувального центру після закінчення строку їх чинності з використанням методу, що унеможлиблює їх відновлення.

22. Відповідальні особи Засвідчувального центру зобов'язані знищити свої особисті ключі після закінчення строку їх чинності з використанням методу, що унеможлиблює їх відновлення.

VIII. Сертифікати ключів у Засвідчувальному центрі

1. Засвідчувальний центр формує сертифікати ключів відповідно до Вимог до формату посиленого сертифіката відкритого ключа, затверджених наказом Міністерства юстиції України, Адміністрації Державної служби спеціального зв'язку та захисту інформації України від 20 серпня 2012 року № 1236/5/453, зареєстрованих у Міністерстві юстиції України 20 серпня 2012 року за № 1398/21710 (зі змінами).

2. Центральний засвідчувальний орган формує сертифікати власних ключів Засвідчувального центру для криптографічного алгоритму ДСТУ 4145-2002.

3. Адміністратор сертифікації Засвідчувального центру зобов'язаний забезпечити формування сертифікатів власних ключів Засвідчувального центру для криптографічного алгоритму RSA. Адміністратор сертифікації Засвідчувального центру зобов'язаний забезпечити формування сертифікатів ключів послуги інтерактивного визначення статусу сертифіката ключа та сертифікатів ключів Центрів.

4. Сертифікати власних ключів Засвідчувального центру використовуються для перевірки списків відкликаних сертифікатів ключів

Засвідчувального центру та сертифікатів ключів, сформованих Засвідчувальним центром.

5. Сертифікати ключів послуги інтерактивного визначення статусу сертифіката ключа використовуються виключно для перевірки електронного цифрового підпису під час надання послуги інтерактивного визначення статусу сертифіката ключа, сформованого Засвідчувальним центром.

6. Сертифікати ключів, сформовані в Засвідчувальному центрі для Центру, використовуються для перевірки списку відкликаних сертифікатів ключів Центру та сертифікатів ключів, сформованих Центром.

7. Засвідчувальний центр має право встановлювати обмеження сфери використання сформованих ним сертифікатів ключів. Інформація щодо обмеження сфери їх використання доводиться до відома заявника Центру та зазначається в сертифікаті ключа, сформованого в Засвідчувальному центрі.

8. Строк чинності сертифікатів ключів Засвідчувального центру становить не більше п'яти років. Планова заміна сертифікатів власних ключів Засвідчувального центру здійснюється згідно з вимогами Регламенту роботи центрального засвідчувального органу, затвердженого наказом Міністерства юстиції України від 29 січня 2013 року № 183/5, зареєстрованого в Міністерстві юстиції України 30 січня 2013 року за № 191/22723 (зі змінами). Планова заміна сертифікатів ключів послуги інтерактивного визначення статусу сертифіката ключа здійснюється згідно з вимогами цього Регламенту.

9. Строк чинності сертифіката ключа зареєстрованого Центру становить не більше двох років з дати і часу їх формування в Засвідчувальному центрі, акредитованого Центру – не більше п'яти років.

10. Строк чинності сертифіката ключа закінчується в разі його скасування. Сертифікат ключа тимчасово не є чинним протягом строку його блокування.

ІХ. Порядок подання документів до Засвідчувального центру для проведення регламентних процедур та їх опрацювання

1. Заявник Центру особисто подає до служби реєстрації Засвідчувального центру заяви про реєстрацію, акредитацію, формування сертифіката ключа, зміну статусу сертифіката ключа Центру, унесення змін до реєстраційних даних Центру, видачу дублікату свідоцтва про реєстрацію/акредитацію Центру, договір про надання послуг у паперовій та електронній формах.

2. Адміністратор реєстрації Засвідчувального центру засвідчує заяви про реєстрацію, акредитацію, формування сертифіката ключа, зміну статусу сертифіката ключа Центру, унесення змін до реєстраційних даних Центру,

видачу дубліката свідоцтва про реєстрацію/акредитацію Центру, договір про надання послуг в електронній формі шляхом накладення на них електронного цифрового підпису.

3. Центр у разі зміни особи заявника Центру зобов'язаний повідомити про це Засвідчувальний центр. Новий заявник Центру особисто подає до служби реєстрації Засвідчувального центру:

засвідчену в установленому порядку копію паспорта заявника Центру;
засвідчену в установленому порядку довіреність заявника Центру.

4. Служба реєстрації Засвідчувального центру приймає заяви про реєстрацію/акредитацію Центру за наявності всіх документів, визначених цим Регламентом для здійснення зазначених процедур.

5. Всі заяви мають бути заповнені українською мовою, розбірливо, друкованими літерами, без виправлень. Служба реєстрації Засвідчувального центру не приймає на розгляд документи, які містять виправлення, дописки, закреслені слова, написи, а також пошкодження, унаслідок яких їх текст не можна прочитати.

6. Адміністратор реєстрації Засвідчувального центру виконує процедуру ідентифікації (установлення особи) заявника Центру під час отримання заяв про реєстрацію, акредитацію, формування сертифіката ключа, зміну статусу сертифіката ключа Центру, унесення змін до реєстраційних даних Центру, видачу дубліката свідоцтва про реєстрацію/акредитацію Центру. Установлення особи заявника Центру здійснюється за паспортом або документом, що його замінює.

7. Заявник Центру разом із заявою зобов'язаний подати адміністраторові реєстрації Засвідчувального центру засвідчену в установленому порядку довіреність, що підтверджує його повноваження діяти від імені Центру під час організації та проведення регламентних процедур в Засвідчувальному центрі.

8. Підставою для обробки персональних даних у Засвідчувальному центрі є згода суб'єктів персональних даних на обробку їх персональних даних. Така згода оформляється у вигляді письмового дозволу на обробку персональних даних (додаток 9), у якому задокументовано добровільне волевиявлення фізичних осіб щодо надання дозволу на обробку їх персональних даних. Дозвіл на обробку персональних даних надають ті суб'єкти персональних даних, чий персональні дані вперше передаються до Засвідчувального центру для проведення відповідної регламентної процедури. Заявник Центру подає адміністраторові реєстрації Засвідчувального центру дозвіл на обробку персональних даних разом із відповідною заявою.

9. Адміністратор реєстрації Засвідчувального центру зобов'язаний взяти на облік усі документи, що були подані заявником Центру під час проведення всіх регламентних процедур, шляхом формування справи Центру та внесення необхідних даних Центру до реєстру Засвідчувального центру.

10. Адміністратор реєстрації Засвідчувального центру зобов'язаний перевірити повноту комплекту поданих заявником Центру документів для проведення відповідної регламентної процедури, правильність їх оформлення і відповідність законодавству України у сфері електронного цифрового підпису.

11. Служба реєстрації Засвідчувального центру за результатом розгляду поданих документів відмовляє в проведенні відповідної регламентної процедури, якщо:

- немає необхідних для проведення цієї регламентної процедури документів;
- подано неналежним чином засвідчені копії документів;
- установлено невідповідність даних, що зазначені в поданих документах, фактичним.

12. Служба реєстрації Засвідчувального центру повертає заявникові Центру подані ним документи в разі відмови в проведенні регламентної процедури. Адміністратор реєстрації Засвідчувального центру зазначає підстави для відмови в проведенні регламентної процедури у відповідній заяві в паперовій формі.

13. Центр подає до Засвідчувального центру такі види документів:
засвідчені копії документів на паперовому носії;
оригінали документів на паперовому (з необхідним підписами та печатками) та електронному носіях.

14. Адміністратор реєстрації Засвідчувального центру в разі подання засвідченої копії документа на паперовому носії зобов'язаний:

- перевести засвідчену копію документа на паперовому носії в електронний вигляд шляхом сканування;
- підшити копії документа на паперовому носії у справу;
- унести до бази даних електронний варіант відсканованої копії документа.

15. Адміністратор реєстрації Засвідчувального центру в разі подання оригіналу документа на паперовому (з необхідними підписами та печатками) та електронному носіях зобов'язаний:

- перевести оригінал документа на паперовому носії в електронний вигляд шляхом сканування;
- підшити оригінал документа на паперовому носії до справи;
- унести до бази даних електронний документ, електронний варіант відсканованого оригіналу.

16. Адміністратор реєстрації Засвідчувального центру зобов'язаний зберігати справи в сейфі/ящику/шафі, що надійно замикається і до якого(ї) не мають доступу сторонні особи, та несе особисту відповідальність за їх надійне зберігання.

17. Адміністратор реєстрації Засвідчувального центру зобов'язаний здійснити порівняння ідентифікаційних даних Центру в заяві про формування сертифіката ключа Центру в Засвідчувальному центрі чи про зміну статусу сертифіката ключа Центру з даними, занесеними до реєстру Засвідчувального центру.

18. Адміністратор реєстрації Засвідчувального центру зобов'язаний здійснити порівняння ідентифікаційних даних Центру, наведених у заявах про формування сертифіката ключа Центру в Засвідчувальному центрі і про внесення змін до реєстраційних даних зареєстрованого/акредитованого Центру в Засвідчувальному центрі, з даними, що містяться в копіях документів, які підтверджують ці зміни, якщо формування нового сертифіката ключа відбувається у зв'язку зі зміною ідентифікаційних даних Центру, які внесені до реєстру Засвідчувального центру.

Х. Реєстрація Центру

1. Заявник Центру для здійснення реєстрації Центру в Засвідчувальному центрі зобов'язаний подати такі документи:

заяву про реєстрацію Центру в Засвідчувальному центрі;

заяву про формування сертифіката ключа Центру в Засвідчувальному центрі;

засвідчені в установленому порядку копії установчих документів (надаються Центром, що є окремою юридичною особою);

засвідчену в установленому порядку копію документа, що підтверджує створення Центру;

засвідчені в установленому порядку копії документів про призначення керівника Центру, заступника(ів) керівника Центру, відповідальних осіб Центру;

засвідчені в установленому порядку копії паспортів заявника, керівника/заступника(ів) керівника Центру;

засвідчену в установленому порядку довіреність заявника Центру;

засвідчену в установленому порядку копію регламенту роботи Центру;

засвідчену в установленому порядку копію положення, у якому визначаються функціональні обов'язки відповідальних осіб Центру;

засвідчену в установленому порядку копію порядку синхронізації із Всесвітнім координованим часом;

засвідчені в установленому порядку копії ліцензій на право проведення господарської діяльності в галузі криптографічного або технічного захисту інформації (за наявності);

фразу-пароль для блокування сертифіката ключа по телефону (у запечатаному конверті, на якому надруковано адресу Центру та телефони для зв'язку).

2. Строк розгляду заяви про реєстрацію Центру в Засвідчувальному центрі становить не більше семи робочих днів від дати її прийняття.

3. Засвідчувальний центр після подання заявником Центру документів проводить реєстрацію Центру в такому порядку:

1) адміністратор реєстрації Засвідчувального центру опрацьовує подані документи згідно з вимогами, визначеними в розділі IX цього Регламенту;

2) Засвідчувальний центр приймає рішення про реєстрацію/відмову в реєстрації Центру в Засвідчувальному центрі;

3) адміністратор реєстрації Засвідчувального центру в разі ухвалення рішення про реєстрацію Центру в Засвідчувальному центрі формує унікальне розпізнавальне ім'я Центру згідно з вимогами, визначеними розділом XIII цього Регламенту, та вносить до реєстру Засвідчувального центру реєстраційні дані Центру;

4) адміністратор сертифікації Засвідчувального центру в разі ухвалення рішення про реєстрацію Центру в Засвідчувальному центрі змінює статус Центру на зареєстрований із зазначенням дати прийняття та номера відповідного рішення про реєстрацію;

5) адміністратор реєстрації Засвідчувального центру вносить до бази даних Засвідчувального центру відкритий ключ Центру для засвідчення його чинності;

6) адміністратор сертифікації Засвідчувального центру формує сертифікат ключа Центру і поширює його та дані про статус Центру згідно з вимогами, визначеними цим Регламентом.

4. Служба реєстрації Засвідчувального центру зобов'язана надрукувати свідоцтво про реєстрацію Центру встановленого зразка і надати заявникові Центру це свідоцтво протягом п'яти робочих днів від дати внесення до реєстру Засвідчувального центру запису про реєстрацію Центру.

XI. Акредитація Центру

1. Центр для одержання статусу акредитованого має бути зареєстрованим Центром у Засвідчувальному центрі і відповідати вимогам, установленим цим

Регламентом, Законом України “Про електронний цифровий підпис” та іншими нормативно-правовими актами у сфері електронного цифрового підпису.

2. Заявник Центру для здійснення акредитації Центру в Засвідчувальному центрі зобов’язаний подати такі документи:

заяву про акредитацію Центру в Засвідчувальному центрі за формою, визначеною в додатку 4;

заяву про формування сертифіката ключа Центру в Засвідчувальному центрі за формою, визначеною в додатку 5;

документи, перелік яких наведено в пункті 1 розділу X цього Регламенту;

засвідчені в установленому порядку копії сертифікатів відповідності або позитивних експертних висновків за результатами державної експертизи у сфері криптографічного захисту інформації на засоби криптографічного захисту інформації;

засвідчену в установленому порядку копію атестата відповідності комплексної системи захисту інформації Центру;

засвідчену в установленому порядку копію документа “План-схема приміщень Центру та порядок доступу до спеціальних приміщень”;

засвідчену в установленому порядку копію документа “Порядок зберігання окремих резервних копій сертифікатів ключів та списку відкликаних сертифікатів, сформованих акредитованим Центром”;

засвідчену в установленому порядку копію Положення про службу захисту інформації Центру.

3. Засвідчувальний центр у процесі проведення акредитації Центру здійснює перевірку Центру на відповідність вимогам, визначеним нормативно-правовими актами Національного банку України, з урахуванням регламенту роботи Центру.

4. Строк розгляду заяви про акредитацію Центру в Засвідчувальному центрі становить не більше 45 робочих днів від дати її надходження.

5. Засвідчувальний центр після подання заявником Центру документів проводить акредитацію Центру в такому порядку:

1) адміністратор реєстрації Засвідчувального центру опрацьовує подані документи згідно з вимогами, визначеними в розділі IX цього Регламенту;

2) Засвідчувальний центр приймає рішення про акредитацію/відмову в акредитації Центру в Засвідчувальному центрі;

3) адміністратор сертифікації Засвідчувального центру в разі ухвалення рішення про акредитацію змінює статус Центру на акредитований із зазначенням дати прийняття та номера відповідного рішення про акредитацію;

4) адміністратор реєстрації Засвідчувального центру вносить до бази даних Засвідчувального центру відкритий ключ Центру для засвідчення його чинності;

5) адміністратор сертифікації Засвідчувального центру формує сертифікат ключа Центру і поширює його та дані про статус Центру згідно з вимогами, визначеними цим Регламентом.

6. Служба реєстрації Засвідчувального центру зобов'язана надрукувати свідоцтво про акредитацію Центру устанавленого зразка зі строком дії п'ять років з дати прийняття рішення про акредитацію і надати заявникові Центру це свідоцтво протягом п'яти робочих днів від дати внесення до реєстру Засвідчувального центру запису про акредитацію Центру.

7. Акредитований Центр проходить повторну акредитацію згідно з вимогами щодо процедури акредитації Центру, визначеними цим Регламентом, у таких випадках:

зміна основних даних (реквізитів), які зазначаються у свідоцтві про акредитацію;

закінчення строку дії свідоцтва про акредитацію;

втрата чинності чи закінчення строку дії атестата відповідності комплексної системи захисту інформації в разі відсутності нового атестата відповідності або внесення до програмно-технічного комплексу Центру змін, які потребують модернізації комплексної системи захисту інформації;

закінчення строку дії сертифіката відповідності або позитивного експертного висновку за результатами державної експертизи у сфері криптографічного захисту інформації у разі відсутності нового сертифіката/експертного висновку.

XII. Скасування реєстрації/акредитації та припинення діяльності Центру

1. Засвідчувальний центр приймає рішення про скасування реєстрації/акредитації Центру в таких випадках:

виявлення порушень вимог, установлених Правилами реєстрації, засвідчення чинності відкритого ключа та акредитації центрів сертифікації ключів банків України в Засвідчувальному центрі Національного банку України, затвердженими постановою Правління Національного банку України від 17 червня 2010 року № 284, зареєстрованими в Міністерстві юстиції України 04 листопада 2010 року за № 1035/18330 (зі змінами), іншими нормативно-правовими актами Національного банку України та законодавством у сфері електронного цифрового підпису;

прийняття Центром рішення про припинення своєї діяльності.

2. Засвідчувальний центр зобов'язаний оприлюднити інформацію про рішення щодо скасування реєстрації/акредитації Центру протягом трьох робочих днів після прийняття такого рішення шляхом:

розміщення інформації про це рішення на інформаційному ресурсі Засвідчувального центру;

повідомлення про це рішення Центру із зазначенням підстав скасування.

3. Центр зобов'язаний повідомити Засвідчувальний центр про рішення щодо припинення своєї діяльності за три місяці до припинення діяльності.

Засвідчувальний центр зобов'язаний розмістити інформацію про рішення щодо припинення діяльності Центру на інформаційному ресурсі Засвідчувального центру протягом трьох робочих днів після одержання від Центру повідомлення про рішення щодо припинення своєї діяльності.

4. Зареєстрований Центр не має права формувати нові сертифікати відкритих ключів після оприлюднення інформації про рішення щодо скасування його реєстрації чи припинення діяльності.

Акредитований Центр не має права формувати нові сертифікати ключів після оприлюднення інформації про рішення щодо скасування його акредитації чи припинення діяльності.

5. Засвідчувальний центр скасовує реєстрацію/акредитацію Центру через три місяці після прийняття рішення щодо скасування реєстрації/акредитації Центру або одержання від Центру повідомлення про рішення щодо припинення своєї діяльності.

6. Центр у разі скасування його реєстрації/акредитації чи припинення діяльності зобов'язаний передати документовану інформацію на зберігання Засвідчувальному центру.

7. Адміністратор сертифікації Засвідчувального центру після приймання документованої інформації зобов'язаний скасувати сертифікати ключів Центру та поширити інформацію про зміну статусу сертифіката ключа Центру в порядку, установленому цим Регламентом.

8. Адміністратор сертифікації Засвідчувального центру після скасування реєстрації Центру зобов'язаний змінити статус зареєстрованого Центру на "збережений". Засвідчувальний центр після скасування реєстрації Центру вносить його до списку Центрив, що припинили діяльність.

9. Адміністратор сертифікації Засвідчувального центру зобов'язаний змінити статус Центру на "зареєстрований" після скасування його акредитації.

Центр після скасування його акредитації має право подати до Засвідчувального центру відкритий ключ Центру для засвідчення його чинності у встановленому порядку.

У разі неподання Центром свого відкритого ключа для засвідчення його чинності протягом трьох місяців з дати скасування акредитації Центру Засвідчувальний центр вносить Центр до списку Центрив, що припинили діяльність.

10. Адміністратор сертифікації Засвідчувального центру після зміни статусу Центру чи припинення діяльності Центру зобов'язаний поширити інформацію про зміну статусу Центру в порядку, установленому цим Регламентом.

XIII. Формування унікального розпізнавального імені Центру

1. Адміністратор реєстрації Засвідчувального центру формує унікальне розпізнавальне ім'я Центру під час унесення даних про Центр до реєстру Засвідчувального центру. Його унікальність забезпечується шляхом додавання до розпізнавального імені Центру реквізиту “серійний номер” (поле “SERIALNUMBER”).

2. Реквізит “серійний номер” для Центру складається з таких елементів:

UA-[код установи]{-[Додаток]},

де UA – код України;

код установи – ідентифікаційний код юридичної особи за ЄДРПОУ;

додаток – необов'язкова послідовність від однієї до чотирьох цифр, що містить додаткову частину ідентифікатора.

XIV. Формування унікального розпізнавального імені відповідальної особи Засвідчувального центру

1. Адміністратор безпеки Засвідчувального центру формує унікальне розпізнавальне ім'я відповідальної особи Засвідчувального центру під час унесення її даних до реєстру Засвідчувального центру. Забезпечення його унікальності відбувається шляхом додавання до розпізнавального імені відповідальної особи Засвідчувального центру (прізвище, ім'я, по батькові) реквізиту “серійний номер” (поле “SERIALNUMBER”).

2. Реквізит “серійний номер” для відповідальної особи Засвідчувального центру складається з таких елементів:

UA-[код структурного підрозділу][табельний номер]{-[Додаток]},

де UA – код України;

код структурного підрозділу – два символи коду структурного підрозділу, які визначаються Правилами кодування підрозділів Національного банку України та визначення ідентифікаторів його працівників, затвердженими постановою Правління Національного банку України від 19 травня 2004 року № 228;

табельний номер – чотири цифри, що містять табельний номер працівника Національного банку України;

додаток – необов'язкова послідовність від однієї до чотирьох цифр, що містить додаткову частину ідентифікатора.

XV. Формування сертифіката ключа Центру

1. Засвідчувальний центр здійснює формування сертифіката ключа Центру на підставі заяви про формування сертифіката ключа Центру в Засвідчувальному центрі. Служба реєстрації Засвідчувального центру приймає заяву лише під час реєстрації/акредитації Центру або від зареєстрованого/акредитованого Центру.

2. Заявник Центру подає Засвідчувальному центру разом із заявою про формування сертифіката ключа Центру в Засвідчувальному центрі запит на формування сертифіката ключа Центру в електронному вигляді. Запит може бути двох видів:

у форматі PKCS#10 з накладеним електронним цифровим підписом з використанням особистого ключа Центру;
самопідписаний сертифікат ключа Центру.

3. Засвідчувальний центр формує сертифікати ключів Центру для відкритих ключів, що згенеровані відповідно до криптографічних алгоритмів ДСТУ 4145-2002 та RSA.

4. Засвідчувальний центр здійснює формування сертифіката ключа Центру на підставі даних, отриманих від Центру під час його реєстрації/акредитації, і даних, що містяться в запиті на формування сертифіката ключа.

5. Строк розгляду заяви про формування сертифіката ключа зареєстрованого/акредитованого Центру в Засвідчувальному центрі становить не більше трьох робочих днів від дати її прийняття.

6. Засвідчувальний центр під час формування сертифіката ключа Центру виконує такі дії:

визначає дату, час початку та закінчення строку чинності сертифіката ключа;

уносить до сертифіката ключа Центру обов'язкові дані, визначені Законом України "Про електронний цифровий підпис";

уносить до сертифіката ключа Центру додаткові дані за зверненням Центру;

уносить до сертифіката ключа Центру інформацію щодо місця розміщення списку відкликаних сертифікатів Засвідчувального центру на інформаційному ресурсі Засвідчувального центру;

забезпечує унікальність реєстраційного номера сертифіката ключа в межах Засвідчувального центру, а також контролює унікальність відкритого ключа Центру та унікальність розпізнавального імені Центру в реєстрі Засвідчувального центру.

7. Служба реєстрації Засвідчувального центру за результатами розгляду поданих Центром документів для формування сертифіката ключа Центру приймає рішення про відмову у формуванні сертифіката ключа Центру, якщо: виявлено хоча б одну з умов, зазначених у пункті 11 розділу IX Регламенту;

запит на формування сертифіката ключа не відповідає вимогам, визначеним пунктом 2 цього розділу;

поле “серійний номер” (“SERIALNUMBER”) у запиті на формування сертифіката ключа Центру не відповідає вимогам, визначеним пунктом 2 розділу XIII Регламенту;

особистий та відкритий ключі не відповідають вимогам, визначеним пунктами 6, 7 розділу VII цього Регламенту та пунктом 3 цього розділу.

8. Засвідчувальний центр здійснює формування сертифіката ключа Центру в такому порядку:

1) адміністратор реєстрації Засвідчувального центру опрацьовує подані документи згідно з вимогами розділу IX цього Регламенту;

2) Засвідчувальний центр приймає рішення про формування/відмову у формуванні сертифіката ключа Центру;

3) адміністратор реєстрації Засвідчувального центру вносить до бази даних поданий заявником Центру запит на формування сертифіката ключа Центру (самопідписаний сертифікат ключа Центру);

4) адміністратор реєстрації Засвідчувального центру здійснює засобами програмно-технічного комплексу Засвідчувального центру перевірку електронного цифрового підпису в запиті на формування сертифіката ключа Центру (у самопідписаному сертифікаті ключа Центру). Запит на формування сертифіката ключа Центру (самопідписаний сертифікат ключа Центру) вноситься до бази даних лише в разі підтвердження електронного цифрового підпису;

5) адміністратор сертифікації Засвідчувального центру формує сертифікат ключа Центру в електронній формі. Адміністратор сертифікації Засвідчувального центру під час формування сертифіката ключа Центру виконує вимоги пункту 6 цього розділу;

6) заявник Центру після формування сертифіката ключа Центру зобов'язаний перевірити правильність відомостей, що містяться в кожному сертифікаті ключа Центру. У разі виявлення некоректних даних (помилки в реквізитах) він зобов'язаний повідомити про зазначене адміністратора реєстрації Засвідчувального центру. У цьому разі адміністратор сертифікації

Засвідчувального центру скасовує сертифікат ключа Центру та формує новий сертифікат ключа Центру;

7) адміністратор сертифікації Засвідчувального центру вносить зміни до реєстру чинних сертифікатів ключів Центрів і здійснює поширення сертифіката ключа Центру в спосіб, визначений пунктом 1 розділу XXIII Регламенту.

9. Центр має подати до Засвідчувального центру заяву про формування нового сертифіката ключа Центру не пізніше ніж за десять робочих днів до закінчення строку чинності його поточного сертифіката ключа. У разі неотримання від Центру заяви про формування нового сертифіката ключа Центру у визначений термін Засвідчувальний центр після закінчення строку чинності сертифіката ключа Центру приймає рішення про скасування реєстрації/акредитації.

10. Центр має право подавати до Засвідчувального центру на сертифікацію попередньо засвідчений відкритий ключ Центру протягом строку чинності сертифіката ключа, якщо відповідний йому особистий ключ не був скомпрометований. У такому випадку дата і час закінчення строку чинності нового сертифіката ключа Центру, сформованого на основі попередньо засвідченого відкритого ключа Центру, не може перевищувати дати і часу закінчення строку чинності попереднього сертифіката ключа Центру.

11. Програмно-технічний комплекс Засвідчувального центру в момент закінчення строку чинності сертифіката ключа Центру:

автоматично скасовує поточний сертифікат ключа Центру;

формує та поширює список відкликаних сертифікатів ключів Засвідчувального центру.

XVI. Формування сертифікатів власних ключів Засвідчувального центру

1. Адміністратор сертифікації Засвідчувального центру здійснює генерування відкритих та особистих власних ключів Засвідчувального центру в спосіб, визначений цим Регламентом та інструкціями щодо роботи з ключовими даними. Відразу після генерування ключів автоматично створюються запити на формування сертифікатів ключів у форматі PKCS#10 та самопідписані сертифікати ключів для криптографічних алгоритмів ДСТУ 4145-2002 та RSA.

2. Адміністратор сертифікації Засвідчувального центру вивантажує запит на формування сертифіката ключа у форматі PKCS#10 та самопідписаний сертифікат ключа для криптографічного алгоритму ДСТУ 4145-2002 з АКЗЗІ і подає до центрального засвідчувального органу разом з документами, визначеними Регламентом роботи центрального засвідчувального органу, затвердженим наказом Міністерства юстиції України 29 січня 2013 року

№ 183/5, зареєстрованим в Міністерстві юстиції України 30 січня 2013 року за № 191/22723 (зі змінами).

3. Адміністратор сертифікації Засвідчувального центру отримує сформований в Центральному засвідчувальному органі сертифікат ключа для криптографічного алгоритму ДСТУ 4145-2002 і здійснює активування ключів для криптографічних алгоритмів ДСТУ 4145-2002 та RSA в спосіб, визначений інструкціями щодо роботи з ключовими даними.

4. Адміністратор сертифікації Засвідчувального центру здійснює поширення сертифікатів власних ключів Засвідчувального центру в спосіб, визначений цим Регламентом.

XVII. Формування сертифікатів ключів послуги інтерактивного визначення статусу сертифіката ключа

1. Формування сертифікатів ключів послуги інтерактивного визначення статусу сертифіката ключа здійснюється в такому порядку:

1) адміністратор сертифікації Засвідчувального центру здійснює генерування відкритих та особистих ключів послуги інтерактивного визначення статусу сертифіката ключа в спосіб, визначений цим Регламентом та інструкціями щодо роботи з ключовими даними. Адміністратор сертифікації Засвідчувального центру формує сертифікати ключів послуги інтерактивного визначення статусу сертифіката ключа для криптографічних алгоритмів ДСТУ 4145-2002 та RSA;

2) адміністратор сертифікації Засвідчувального центру здійснює активування ключів послуги інтерактивного визначення статусу сертифіката ключа для криптографічних алгоритмів ДСТУ 4145-2002 та RSA в спосіб, визначений інструкціями щодо роботи з ключовими даними;

3) адміністратор сертифікації Засвідчувального центру здійснює поширення сертифікатів ключів послуги інтерактивного визначення статусу сертифіката ключа в спосіб, визначений цим Регламентом.

2. Адміністратор сертифікації Засвідчувального центру не пізніше ніж за десять робочих днів до закінчення строку чинності поточного сертифіката ключа генерує нові криптографічні ключі та здійснює процедуру формування нового сертифіката ключа послуги інтерактивного визначення статусу сертифіката ключа.

XVIII. Зміна статусу сертифіката ключа Центру

1. Засвідчувальний центр блокує/поновлює сертифікат ключа Центру в разі:

подання заяви про блокування/поновлення сертифіката ключа Центру від заявника Центру до служби реєстрації Засвідчувального центру за формою, визначеною в додатку 2 до цього Регламенту;
наявності рішення суду, що набрало законної сили.

2. Засвідчувальний центр скасовує сертифікат ключа Центру в разі:
закінчення строку чинності сертифіката ключа Центру;
компрометації особистого ключа Центру;
подання заяви про скасування сертифіката ключа Центру від заявника Центру до служби реєстрації Засвідчувального центру за формою, визначеною в додатку 2 до цього Регламенту;
наявності рішення суду, що набрало законної сили;
надання заявником Центру недостовірних даних;
скасування реєстрації/акредитації Центру;
припинення діяльності Центру.

3. Центр зобов'язаний звернутися до служби реєстрації Засвідчувального центру щодо блокування/скасування сертифіката ключа внаслідок виявлення даних про:
втрату або компрометацію особистого ключа Центру;
втрату контролю за особистим ключем Центру через компрометацію пароля (коду, персонального ідентифікаційного номера), доступу до нього;
зміну відомостей, зазначених у сертифікаті ключа Центру.

4. Центр має право звернутися до служби реєстрації Засвідчувального центру щодо поновлення сертифіката ключа внаслідок виявлення недостовірності даних про:
втрату або компрометацію особистого ключа Центру;
втрату контролю за особистим ключем Центру через компрометацію пароля (коду, персонального ідентифікаційного номера), доступу до нього;
зміну відомостей, зазначених у сертифікаті ключа Центру.

5. Заявник Центру має право подати адміністраторові реєстрації Засвідчувального центру заяву про блокування сертифіката ключа Центру в усній формі по телефону. У цій заяві мають зазначатися:
ідентифікаційні дані Центру – власника сертифіката ключа;
ідентифікаційні дані заявника Центру;
серійний номер сертифіката ключа Центру, що блокується;
причина блокування;
строк, на який блокується сертифікат ключа Центру;
фраза-пароль (обумовлена в процесі реєстрації/акредитації Центру).

Засвідчувальний центр здійснює блокування сертифіката ключа Центру за заявою в усній формі тільки в разі позитивної автентифікації Центру (відповідність ідентифікаційних даних Центру, заявника Центру, серійного

номера сертифіката ключа Центру та фрази-пароля, переданої в усній заяві, інформації з реєстру Засвідчувального центру).

6. Центр зобов'язаний підтвердити заяву про блокування сертифіката ключа Центру в усній формі письмовою заявою про блокування сертифіката ключа Центру за формою, визначеною в додатку 2 до цього Регламенту, протягом двох робочих днів з дати прийняття Засвідчувальним центром заяви в усній формі. У разі ненадходження відповідної письмової заяви, що підтверджує блокування сертифіката ключа Центру, протягом зазначеного строку Засвідчувальний центр блокує сертифікат ключа цього Центру строком на один календарний місяць.

7. Засвідчувальний центр під час зміни статусу сертифіката ключа Центру вносить відповідні зміни до реєстру Засвідчувального центру та списку відкликаних сертифікатів Засвідчувального центру із зазначенням дати, часу та причин зміни статусу сертифіката ключа Центру.

8. Зміна статусу сертифіката ключа Центру набирає чинності з моменту внесення відповідних змін до реєстру Засвідчувального центру та списку відкликаних сертифікатів ключів Засвідчувального центру.

9. Засвідчувальний центр зобов'язаний опрацювати заяву про зміну статусу сертифіката ключа Центру протягом не більше двох годин з моменту її подання.

10. Засвідчувальний центр здійснює зміну статусу сертифіката ключа Центру в такому порядку:

1) адміністратор реєстрації Засвідчувального центру:
опрацьовує подані документи згідно з вимогами розділу IX цього Регламенту;

створює запит на зміну статусу поточного сертифіката ключа Центру;

2) адміністратор сертифікації Засвідчувального центру:
засвідчує запит на зміну статусу поточних сертифіката ключа Центру;
формує список відкликаних сертифікатів ключів Засвідчувального центру;
поширює інформацію про зміну статусу сертифіката ключа Центру в порядку, установленому пунктами 1 – 3 розділу XXIII цього Регламенту.

XIX. Зміна статусу сертифіката власного ключа Засвідчувального центру

1. Зміна статусу сертифіката власного ключа Засвідчувального центру для криптографічного алгоритму ДСТУ 4145-2002 набирає чинності з моменту внесення відповідних змін до реєстру центрального засвідчувального органу та

списку відкликаних сертифікатів ключів, сформованого центральним засвідчувальним органом.

Зміна статусу сертифіката власного ключа Засвідчувального центру для криптографічного алгоритму RSA набирає чинності з моменту внесення відповідних змін до реєстру Засвідчувального центру.

2. Керівник/заступник керівника Засвідчувального центру зобов'язаний установити термін блокування сертифіката власного ключа Засвідчувального центру. Цей термін не може перевищувати строку, визначеного законодавством у сфері електронного цифрового підпису.

3. Адміністратор сертифікації Засвідчувального центру в разі зміни статусу сертифіката власного ключа Засвідчувального центру для криптографічного алгоритму ДСТУ 4145-2002 зобов'язаний подати заяву про зміну статусу поточного сертифіката власного ключа Засвідчувального центру до центрального засвідчувального органу відповідно до вимог Регламенту роботи центрального засвідчувального органу, затвердженого наказом Міністерства юстиції України 29 січня 2013 року № 183/5, зареєстрованого в Міністерстві юстиції України 30 січня 2013 року за № 191/22723 (зі змінами).

4. Адміністратор сертифікації Засвідчувального центру в разі зміни статусу сертифіката власного ключа Засвідчувального центру зобов'язаний поширити інформацію про зміну статусу сертифіката власного ключа Засвідчувального центру згідно з вимогами цього Регламенту.

5. Адміністратор сертифікації Засвідчувального центру в разі скасування сертифіката власного ключа Засвідчувального центру зобов'язаний забезпечити формування нового сертифіката власного ключа відповідно до розділу XVI цього Регламенту.

6. Документи, що були підставою для зміни статусу сертифіката власного ключа Засвідчувального центру, зберігаються в центральному засвідчувальному органі та/або в Засвідчувальному центрі.

XX. Зміна статусу сертифіката ключа послуги інтерактивного визначення статусу сертифіката ключа

1. Зміна статусу сертифіката ключа послуги інтерактивного визначення статусу сертифіката ключа набирає чинності з моменту внесення відповідних змін до реєстру Засвідчувального центру та списку відкликаних сертифікатів ключів Засвідчувального центру.

2. Адміністратор сертифікації Засвідчувального центру зобов'язаний установити термін блокування сертифіката ключа послуги інтерактивного визначення статусу сертифіката ключа. Цей термін не може перевищувати

одного календарного місяця. Поновлення сертифіката ключа послуги інтерактивного визначення статусу сертифіката ключа можливе лише для сертифіката ключа, що заблокований і термін блокування якого не закінчився. Якщо до закінчення терміну блокування сертифіката ключа він не був поновлений, то адміністратор сертифікації Засвідчувального центру зобов'язаний скасувати цей сертифікат ключа.

3. Адміністратор сертифікації Засвідчувального центру має право скасувати сертифікат ключа послуги інтерактивного визначення статусу сертифіката ключа без його блокування.

4. Адміністратор сертифікації Засвідчувального центру зобов'язаний негайно заблокувати/скасувати сертифікат ключа послуги інтерактивного визначення статусу сертифіката ключа в разі:

втрати або компрометації особистого ключа послуги інтерактивного визначення статусу сертифіката ключа;

втрати контролю за особистим ключем послуги інтерактивного визначення статусу сертифіката ключа через компрометацію пароля доступу;

зміни відомостей, зазначених у сертифікаті ключа послуги інтерактивного визначення статусу сертифіката ключа (зокрема у зв'язку зі зміною даних Засвідчувального центру чи зміною налаштувань під час надання відповідних послуг).

5. Адміністратор сертифікації Засвідчувального центру зобов'язаний протягом двох годин поновити сертифікат ключа послуги інтерактивного визначення статусу сертифіката ключа в разі виявлення недостовірності даних про:

втрату або компрометацію особистого ключа послуги інтерактивного визначення статусу сертифіката ключа;

втрату контролю за особистим ключем послуги інтерактивного визначення статусу сертифіката ключа через компрометацію пароля доступу;

зміну відомостей, зазначених у сертифікаті ключа послуги інтерактивного визначення статусу сертифіката ключа.

6. Адміністратор сертифікації Засвідчувального центру під час зміни статусу сертифіката ключа послуги інтерактивного визначення статусу сертифіката ключа зобов'язаний:

створити запит на зміну статусу поточного сертифіката ключа послуги інтерактивного визначення статусу сертифіката ключа та засвідчити його;

унести відповідні зміни до реєстру Засвідчувального центру із зазначенням дати, часу та причин зміни статусу сертифіката ключа послуги інтерактивного визначення статусу сертифіката ключа;

сформувати список відкликаних сертифікатів ключів Засвідчувального центру;

поширити інформацію про зміну статусу сертифіката ключа послуги інтерактивного визначення статусу сертифіката ключа згідно з вимогами цього Регламенту.

7. Адміністратор сертифікації Засвідчувального центру зобов'язаний виконати зміну статусу сертифіката ключа послуги інтерактивного визначення статусу сертифіката ключа протягом однієї години після прийняття цього рішення.

8. Документи, що були підставою для зміни статусу сертифіката ключа послуги інтерактивного визначення статусу сертифіката ключа, зберігаються в Засвідчувальному центрі.

XXI. Блокування/розблокування облікових записів відповідальних осіб Засвідчувального центру

1. Автоматизоване робоче місце адміністратора безпеки Засвідчувального центру забезпечує можливість блокування облікового запису відповідальної особи Засвідчувального центру. У разі блокування облікового запису відповідальної особи Засвідчувального центру ця відповідальна особа Засвідчувального центру не має можливості працювати в програмно-технічному комплексі Засвідчувального центру.

2. Блокування облікового запису відповідальної особи Засвідчувального центру відбувається в разі:

подання відповідальною особою Засвідчувального центру заяви про блокування свого облікового запису;

закінчення строку чинності особистого та відкритого ключів відповідальної особи Засвідчувального центру, якщо нові криптографічні ключі цієї відповідальної особи Засвідчувального центру ще не введено в експлуатацію.

3. Відповідальна особа Засвідчувального центру зобов'язана звернутися до служби захисту інформації Засвідчувального центру щодо блокування свого облікового запису в разі:

компрометації особистого ключа, що зберігається в АКЗЗІ цієї відповідальної особи Засвідчувального центру;

втрати контролю за особистим ключем цієї відповідальної особи Засвідчувального центру через компрометацію пароля доступу до нього;

виходу з ладу (фізичне пошкодження, збої під час роботи тощо) АКЗЗІ цієї відповідальної особи Засвідчувального центру;

втрати АКЗЗІ цією відповідальною особою Засвідчувального центру.

4. Відповідальна особа Засвідчувального центру зобов'язана звернутися до служби захисту інформації Засвідчувального центру щодо розблокування свого облікового запису в разі виявлення недостовірності даних про:

компрометацію особистого ключа, записаного в АКЗЗІ цієї відповідальної особи Засвідчувального центру;

втрату контролю за особистим ключем цієї відповідальної особи Засвідчувального центру через компрометацію пароля доступу до нього;

вихід з ладу (фізичне пошкодження, збої під час роботи тощо) АКЗЗІ цієї відповідальної особи Засвідчувального центру;

втрату АКЗЗІ цією відповідальною особою Засвідчувального центру.

5. Відповідальна особа Засвідчувального центру подає до служби захисту інформації Засвідчувального центру заяву про блокування/розблокування свого облікового запису в усній формі по телефону. У цій заяві зазначаються:

ідентифікаційні дані цієї відповідальної особи Засвідчувального центру;

унікальне розпізнавальне ім'я відповідальної особи Засвідчувального центру;

причина блокування облікового запису;

ключова фраза (обумовлена в процесі створення облікового запису відповідальної особи Засвідчувального центру).

6. Адміністратор безпеки Засвідчувального центру здійснює блокування/розблокування облікового запису відповідальної особи Засвідчувального центру за заявою в усній формі тільки в разі позитивної автентифікації відповідальної особи Засвідчувального центру (збігання наданих у заяві даних з інформацією з реєстру Засвідчувального центру).

XXII. Інформаційний ресурс Засвідчувального центру

1. Інформаційний ресурс Засвідчувального центру призначений для розміщення на ньому відкритої інформації, яка структурно поділяється на:

довідкову інформацію (режим роботи Засвідчувального центру, регламент роботи Засвідчувального центру, нормативно-правові акти з питань застосування електронного цифрового підпису, зразок договору про надання послуг, форми заяв тощо);

дані про Центри;

сертифікати ключів Засвідчувального центру;

сертифікати ключів Центрів;

списки відкликаних сертифікатів Засвідчувального центру;

інше.

2. Засвідчувальний центр зобов'язаний оприлюднити інформацію про набуття Центром статусу зареєстрованого/акредитованого, скасування реєстрації/акредитації Центру та припинення діяльності Центру на інформаційному ресурсі Засвідчувального центру не пізніше ніж наступного робочого дня після внесення відповідних змін у реєстр Засвідчувального центру.

3. Адміністратор сертифікації Засвідчувального центру зобов'язаний розмістити сертифікат власного ключа Засвідчувального центру для криптографічного алгоритму ДСТУ 4145-2002 не пізніше ніж наступного робочого дня після одержання цього сертифіката від центрального засвідчувального органу.

Адміністратор сертифікації Засвідчувального центру зобов'язаний розмістити інші сертифікати ключів Засвідчувального центру на інформаційному ресурсі Засвідчувального центру відразу після їх формування.

4. Розміщення сертифікатів ключів Центру на інформаційному ресурсі Засвідчувального центру здійснюється за згодою Центру. Інформація про потребу оприлюднення сертифіката ключа Центру вноситься до реєстру Засвідчувального центру під час реєстрації/акредитації.

5. Адміністратор сертифікації Засвідчувального центру зобов'язаний розмістити сертифікат ключа Центру на інформаційному ресурсі Засвідчувального центру відразу після його формування та перевірки заявником Центру даних, що внесені до сертифіката ключа Центру.

6. Адміністратор сертифікації Засвідчувального центру зобов'язаний розмістити список відкликаних сертифікатів ключів Засвідчувального центру на інформаційному ресурсі Засвідчувального центру відразу після його формування.

XXIII. Поширення сертифікатів ключів та інформації про статус сертифіката ключа

1. Засвідчувальний центр зобов'язаний розповсюджувати список відкликаних сертифікатів ключів Засвідчувального центру та сертифікати ключів, що сформовані Засвідчувальним центром, шляхом їх розміщення на інформаційному ресурсі Засвідчувального центру і розсилання засобами e-mail та електронної пошти Національного банку України на адреси, що зазначаються в заяві про формування сертифіката ключа Центру в Засвідчувальному центрі.

2. Засвідчувальний центр поширює інформацію про статус сертифіката ключа Центру:

за запитом на інтерактивну перевірку статусу сертифіката ключа з використанням OCSP-сервера;

шляхом розповсюдження списку відкликаних сертифікатів ключів Засвідчувального центру.

3. Взаємодія з OCSP-сервером для визначення статусу сертифікатів ключів забезпечується шляхом використання клієнтського програмного забезпечення. Таке програмне забезпечення повинно відповідати Вимогам до протоколу

визначення статусу сертифіката, затвердженим наказом Міністерства юстиції України, Адміністрації Державної служби спеціального зв'язку та захисту інформації України від 20 серпня 2012 року № 1236/5/453, зареєстрованим в Міністерстві юстиції України 20 серпня 2012 року за № 1403/21715 (зі змінами).

4. Засвідчувальний центр під час формування списку відкликаних сертифікатів ключів Засвідчувального центру зобов'язаний забезпечити:

наявність у списку відкликаних сертифікатів ключів Засвідчувального центру даних щодо часу формування наступного списку відкликаних сертифікатів ключів Засвідчувального центру;

накладення електронного цифрового підпису на список відкликаних сертифікатів ключів Засвідчувального центру за допомогою особистого ключа Засвідчувального центру.

5. Засвідчувальний центр формує списки відкликаних сертифікатів ключів Засвідчувального центру згідно з Вимогами до формату списку відкликаних сертифікатів, затвердженими наказом Міністерства юстиції України, Адміністрації Державної служби спеціального зв'язку та захисту інформації України від 20 серпня 2012 року № 1236/5/453, зареєстрованими в Міністерстві юстиції України 20 серпня 2012 року за № 1400/21712.

Засвідчувальний центр надає інформацію про статус сформованих ним сертифікатів ключів згідно з Вимогами до протоколу визначення статусу сертифіката, затвердженими наказом Міністерства юстиції України, Адміністрації Державної служби спеціального зв'язку та захисту інформації України від 20 серпня 2012 року № 1236/5/453, зареєстрованими в Міністерстві юстиції України 20 серпня 2012 року за № 1403/21715 (зі змінами).

6. Засвідчувальний центр зобов'язаний формувати та розповсюджувати список відкликаних сертифікатів Засвідчувального центру з такою періодичністю:

один раз на добу, навіть якщо протягом останньої доби до списку відкликаних сертифікатів Засвідчувального центру не вносилися зміни,

або після зміни статусу сертифіката ключа, сформованого Засвідчувальним центром.

Наступний список відкликаних сертифікатів Засвідчувального центру може бути сформований раніше визначеного часу його формування.

7. Особа, яка має намір використовувати сертифікат ключа, сформований Засвідчувальним центром, зобов'язана перевірити:

чинність цього сертифіката ключа на момент накладення електронного цифрового підпису на документ;

електронний цифровий підпис у сертифікаті ключа (за допомогою сертифіката власного ключа Засвідчувального центру, чинного на момент формування цього сертифіката ключа);

статус цього сертифіката ключа за списком відкликаних сертифікатів ключів Засвідчувального центру або за запитом на інтерактивну перевірку статусу сертифіката ключа, якщо перевірка здійснюється на момент чинності цього сертифіката ключа;

автентичність і цілісність списку відкликаних сертифікатів ключів Засвідчувального центру та/чи отриманої відповіді служби інтерактивного визначення статусу сертифіката.

8. Якщо одержати інформацію про статус сертифіката ключа, сформованого Засвідчувальним центром, тимчасово неможливо, то потрібно відмовитися від його використання.

XXIV. Синхронізація часу

1. Механізм синхронізації часу програмно-технічного комплексу Засвідчувального центру із Всесвітнім координованим часом (UTC) визначається документом “Порядок синхронізації часу програмно-технічного комплексу Засвідчувального центру із Всесвітнім координованим часом”, що затверджується керівником/заступником керівника Засвідчувального центру.

2. Засвідчувальний центр надає послугу з постачання передачі сигналів точного часу Центрам. Центри повинні синхронізувати час із серверами надання точного часу територіального управління/Центральної розрахункової палати Національного банку України, у яких вони зареєстровані/акредитовані.

3. Центр зобов'язаний розробити Порядок синхронізації часу із Всесвітнім координованим часом та погодити його із Засвідчувальним центром.

XXV. Порядок архівного зберігання документованої інформації

1. Засвідчувальний центр здійснює архівне зберігання: сертифікатів ключів, сформованих Засвідчувальним центром (чинних, скасованих, блокованих), відкритих ключів відповідальних осіб Засвідчувального центру;

реєстру відповідальних осіб Засвідчувального центру, зареєстрованих, акредитованих Центрів та Центрив, що припинили діяльність;

копій і оригіналів документів на паперових носіях та документів на електронних носіях, що подані заявниками Центрив під час проведення регламентних процедур;

списків відкликаних сертифікатів ключів Засвідчувального центру;

запитів на інтерактивну перевірку статусу сертифікатів ключів, сформованих Засвідчувальним центром, та відповідей на ці запити;

журналів аудиту;

documents of information, which is subject to transmission in the event of cancellation of registration, accreditation or termination of activity of the Center.

2. Засвідчувальний центр зберігає документи на паперових носіях у порядку, установленому законодавством України про архіви й архівну справу. Засвідчувальний центр зберігає електронні копії бази даних відповідно до вимог пункту 14 розділу V цього Регламенту. Засвідчувальний центр зберігає електронні копії журналів аудиту відповідно до вимог пункту 10 розділу VI цього Регламенту.

3. Документами постійного зберігання в Засвідчувальному центрі є:
сертифікати ключів, сформовані Засвідчувальним центром;
електронний реєстр сертифікатів ключів Засвідчувального центру;
список відкликаних сертифікатів ключів Засвідчувального центру;
відкриті ключі відповідальних осіб Засвідчувального центру;
сертифікати ключів, сформовані Центрами, що передали документовану інформацію до Засвідчувального центру у зв'язку із скасуванням їх реєстрації/акредитації чи припиненням їх діяльності;
електронні реєстри сертифікатів ключів, сформовані Центрами, що передали документовану інформацію до Засвідчувального центру у зв'язку із скасуванням їх реєстрації/акредитації чи припиненням їх діяльності;
списки відкликаних сертифікатів ключів, сформовані Центрами, що передали документовану інформацію до Засвідчувального центру у зв'язку із скасуванням їх реєстрації/акредитації чи припиненням їх діяльності.

4. Інші документи, що підлягають архівному зберіганню, є документами тимчасового зберігання. Термін зберігання архівних документів становить 10 років.

5. Комісія за безпосередньої участі керівника/заступника керівника Засвідчувального центру та адміністратора безпеки Засвідчувального центру або уповноважених ними відповідальних осіб Засвідчувального центру виконує виділення архівних документів до знищення та їх знищення. За фактом проведення процедури знищення архівних документів складається відповідний акт.

6. Засвідчувальний центр надає доступ до потрібного сертифіката ключа та пов'язаних з ним списків відкликаних сертифікатів ключів з архівних записів Засвідчувального центру за запитом заявників у строки, установлені законодавством України для надання відповідей на звернення громадян.

XXVI. Порядок унесення змін до Регламенту

1. Зміни до цього Регламенту вносяться відповідно до вимог пункту 3.4 Правил посиленої сертифікації, затверджених наказом Департаменту спеціальних телекомунікаційних систем та захисту інформації Служби безпеки України від 13 січня 2005 року № 3, зареєстрованих у Міністерстві юстиції

України 27 січня 2005 року за № 104/10384 (у редакції наказу від 10 травня 2006 року № 50).

2. Засвідчувальний центр інформує Центри та відповідальних осіб Засвідчувального центру про внесення змін до цього Регламенту шляхом надсилання офіційного листа. Регламент зі змінами розміщується на інформаційному ресурсі Засвідчувального центру.

3. Зміни до цього Регламенту обов'язково вносяться в разі внесення змін до законодавства України з питань застосування електронного цифрового підпису. Зміни до цього Регламенту можуть бути внесені у зв'язку з розвитком відповідних інформаційних технологій, появою нових міжнародних і національних стандартів України тощо.

4. Договори та інші правочини, умови яких суперечать унесеним змінам до цього Регламенту, повинні бути переукладені протягом трьох місяців з дня набрання чинності цими змінами.

В. о. начальника
Управління інформаційної безпеки

Д. О. Лук'янов

ПОГОДЖЕНО
Заступник Голови
Національного банку України

_____ Я. В. Смолій
(підпис)

“ ____ ” _____ 20__ року

Додаток 1
до Регламенту роботи Засвідчувального
центру Національного банку України
(пункт 7 розділу I)

Звіт про роботу центру сертифікації ключів
за період з ___ ____ до ___ __

(повне найменування центру сертифікації ключів згідно з ідентифікаційними даними,

унесеними до реєстру Засвідчувального центру Національного банку України)

(свідоцтво про реєстрацію/акредитацію, серія _____ № _____
від “ _____ ” _____ року)

відомості про сертифікати відкритих ключів за весь період існування
центру сертифікації ключів¹:

загальна кількість виданих сертифікатів ключів підписувачів _____;

загальна кількість чинних сертифікатів ключів підписувачів _____;

загальна кількість блокованих сертифікатів ключів підписувачів _____;

загальна кількість скасованих сертифікатів ключів підписувачів _____;

відомості про сертифікати відкритих ключів за звітний період²:

кількість виданих сертифікатів ключів підписувачів _____;

кількість блокувань сертифікатів ключів підписувачів _____;

кількість поновлень сертифікатів ключів підписувачів _____;

кількість скасування сертифікатів ключів підписувачів _____;

кількість скасування сертифікатів ключів підписувачів
без попереднього блокування _____;

¹ Станом на останній день звітнього періоду.

Продовження додатка 1

скарги підписувачів на неправомірну діяльність (або бездіяльність) центру сертифікації ключів:

загальна кількість скарг підписувачів протягом звітного періоду _____.

| № з/п | Опис скарги підписувача | Дії центру сертифікації ключів щодо задоволення/відхилення скарги |
|-------|-------------------------|---|
| | | |
| | | |
| | | |
| | | |

(підпис)

(посада, прізвище, ім'я, по батькові керівника/заступника керівника центру сертифікації ключів)

“ ” _____ року

М. П.

Додаток 2
до Регламенту роботи Засвідчувального
центру Національного банку України
(пункт 7 розділу II)

Заява про зміну статусу
посиленого сертифіката відкритого ключа центру сертифікації ключів

Начальникові Управління Національного банку України
в/у _____ області (Центральної
розрахункової палати Національного банку України)

_____ (прізвище, ім'я, по батькові)

_____ (прізвище, ім'я, по батькові заявника)

_____ серія _____ № _____
(назва документа, що посвідчує особу заявника)

виданий “ _____ ” _____ року

_____ (найменування органу, який видав документ, що посвідчує особу заявника)

що діє на підставі довіреності № _____

від “ _____ ” _____ року,

контактний телефон _____.

Прошу виконати процедуру блокування/скасування/поновлення
посиленого сертифіката відкритого ключа центру сертифікації ключів
відповідно до зазначених відомостей:

_____ (повне найменування центру сертифікації ключів згідно з ідентифікаційними даними,

_____ унесеними до реєстру Засвідчувального центру Національного банку України)

(свідоцтво про реєстрацію/акредитацію, серія _____ № _____

від “ _____ ” _____ року);

унікальний серійний номер центру сертифікації ключів: UA- _____ - _____;

реєстраційний номер посиленого сертифіката відкритого ключа центру сертифікації ключів: _____;

підстави для зміни статусу посиленого сертифіката відкритого ключа центру сертифікації ключів:

_____.

(заповнюється для блокування посиленого сертифіката відкритого ключа).

Строк блокування посиленого сертифіката відкритого ключа центру сертифікації ключів:

початок з “ _____ ” _____ року _____; _____;

(дата) (час)

на період _____

(кількість календарних днів словами)

(заповнюється для поновлення посиленого сертифіката відкритого ключа).

Дата і час блокування посиленого сертифіката відкритого ключа центру сертифікації ключів:

“ _____ ” _____ року _____; _____.

(дата) (час)

(підпис)

(посада, прізвище, ім'я, по батькові керівника/заступника керівника центру сертифікації ключів)

“ _____ ” _____ року

М. П.

Заяву отримано, зареєстровано під № _____, особу заявника центру сертифікації ключів встановлено, відомості, зазначені в заяві, перевірено.

Посилений сертифікат ключа центру сертифікації ключів заблоковано/скасовано/поновлено. Відомості щодо блокування/скасування/поновлення посиленого сертифіката ключа центру сертифікації ключів унесено до реєстру Засвідчувального центру Національного банку України (заповнюється посадовими особами відповідного територіального управління/Центральної розрахункової палати Національного банку України).

Центру сертифікації ключів відмовлено в зміні статусу посиленого сертифіката ключа на підставі (заповнюється посадовими особами відповідного територіального управління/Центральної розрахункової палати Національного банку України в разі відмови в зміні статусу посиленого сертифіката ключа центру сертифікації ключів):

(зазначити підставу для відмови в зміні статусу посиленого сертифіката ключа центру сертифікації ключів)

Рішення про відмову в зміні статусу посиленого сертифіката ключа центру сертифікації ключів № _____ від “ _____ ” _____ року.

(підпис)

(прізвище, ім'я, по батькові начальника територіального управління/Центральної розрахункової палати Національного банку України)

(підпис)

(прізвище, ім'я, по батькові адміністратора реєстрації Засвідчувального центру Національного банку України)

“ _____ ” _____ року

М. П.

Додаток 3
до Регламенту роботи Засвідчувального
центру Національного банку України
(пункт 6 розділу VI)

Заява про реєстрацію центру сертифікації ключів
у Засвідчувальному центрі Національного банку України

Начальникові Управління Національного банку України
в/у _____ області (Центральної
розрахункової палати Національного банку України)

(прізвище, ім'я, по батькові)

(прізвище, ім'я, по батькові заявника)

_____ серія _____ № _____

(назва документа, що посвідчує особу заявника)

виданий “ _____ ” _____ року

(найменування органу, який видав документ, що посвідчує особу заявника)

що діє на підставі довіреності № _____

від “ _____ ” _____ року,

контактний телефон _____.

Прошу внести такі ідентифікаційні дані, зазначені в заяві, до реєстру
Засвідчувального центру Національного банку України:

повне найменування юридичної особи:

_____;

повне найменування центру сертифікації ключів:

_____;

унікальний серійний номер центру сертифікації ключів¹: UA-_____ - ____;

ідентифікаційний код юридичної особи за ЄДРПОУ _____;

організаційно-правова форма _____;

місцезнаходження центру сертифікації ключів:

поштовий індекс _____;

область _____;

район області _____;

населений пункт _____;

вулиця _____;

будинок _____, корпус _____, офіс _____;

телефон _____;

факс _____;

електронна пошта _____;

електронна адреса інформаційного ресурсу _____.

До заяви додаються: _____

(перелік документів, які додаються до заяви)

(підпис)

(посада, прізвище, ім'я, по батькові керівника/заступника керівника
центру сертифікації ключів)

“ _____ ” _____ року

М. П.

¹ Значення цього реквізиту має такий вигляд:

UA-[код установи]{-[додаток]},

де код установи – ідентифікаційний код юридичної особи за ЄДРПОУ;

додаток – необов'язкова послідовність від 1 до 4 цифр, що містить додаткову частину ідентифікатора.

Заяву отримано, зареєстровано під № _____, особу заявника Центру сертифікації ключів встановлено, відомості, зазначені в заяві, перевірено (заповнюється посадовими особами відповідного територіального управління/Центральної розрахункової палати Національного банку України).

Реєстраційні дані, зазначені в заяві, унесено до реєстру Засвідчувального центру Національного банку України, центру сертифікації ключів присвоєно такий унікальний серійний номер: UA-_____ - ____ (заповнюється посадовими особами відповідного територіального управління/Центральної розрахункової палати Національного банку України в разі реєстрації центру сертифікації ключів).

Рішення про реєстрацію № _____ від “ _____ ” _____ року

Свідоцтво про реєстрацію: серія _____ № _____
від “ _____ ” _____ року

Центру сертифікації ключів відмовлено в реєстрації на підставі (заповнюється посадовими особами відповідного територіального управління/Центральної розрахункової палати Національного банку України в разі відмови в реєстрації центру сертифікації ключів):

_____ (зазначити підставу для відмови в реєстрації центру сертифікації ключів)

Рішення про відмову в реєстрації № _____ від “ _____ ” _____ року.

_____ (підпис)

_____ (прізвище, ім'я, по батькові начальника територіального управління/Центральної розрахункової палати Національного банку України)

_____ (підпис)

_____ (прізвище, ім'я, по батькові адміністратора реєстрації Засвідчувального центру Національного банку України)

“ _____ ” _____ року

М. П.

Додаток 4
до Регламенту роботи Засвідчувального
центру Національного банку України
(пункт 6 розділу VI)

Заява про акредитацію центру сертифікації ключів
у Засвідчувальному центрі Національного банку України

Начальникові Управління Національного банку України
в/у _____ області (Центральної
розрахункової палати Національного банку України)

_____ (прізвище, ім'я, по батькові)

_____ (прізвище, ім'я, по батькові заявника)

_____ серія _____ № _____
(назва документа, що посвідчує особу заявника)

виданий “ _____ ” _____ року

_____ (найменування органу, який видав документ, що посвідчує особу заявника)

що діє на підставі довіреності № _____

від “ _____ ” _____ року,

контактний телефон _____.

Прошу провести акредитацію центру сертифікації ключів у
Засвідчувальному центрі Національного банку України з такими
ідентифікаційними даними:

повне найменування юридичної особи:

_____;

повне найменування центру сертифікації ключів:

_____;

унікальний серійний номер центру сертифікації ключів UA-_____ - ____;

ідентифікаційний код юридичної особи за ЄДРПОУ _____;

організаційно-правова форма _____;

свідоцтво про акредитацію¹: серія _____ № _____

від “ ____ ” _____ року;

місцезнаходження центру сертифікації ключів:

поштовий індекс _____;

область _____;

район області _____;

населений пункт _____;

вулиця _____;

будинок _____, корпус _____, офіс _____;

телефон _____;

факс _____;

електронна пошта _____;

електронна адреса інформаційного ресурсу _____.

До заяви додаються: _____

(перелік документів, які додаються до заяви)

_____ (підпис)

_____ (посада, прізвище, ім'я, по батькові керівника/заступника керівника центру сертифікації ключів)

“ ____ ” _____ року

М. П.

¹ Зазначаються відомості про раніше видане свідоцтво (за наявності).

Заяву отримано, зареєстровано під № _____, особу заявника центру сертифікації ключів встановлено, відомості, зазначені в заяві, перевірено (заповнюється посадовими особами відповідного територіального управління/Центральної розрахункової палати Національного банку України).

Акредитацію центру сертифікації ключів проведено (заповнюється посадовими особами відповідного територіального управління/Центральної розрахункової палати Національного банку України в разі акредитації центру сертифікації ключів).

Рішення про акредитацію № _____ від “_____” _____ року

Свідоцтво про акредитацію: серія _____ № _____

від “_____” _____ року

Центру сертифікації ключів відмовлено в акредитації на підставі (заповнюється посадовими особами відповідного територіального управління/Центральної розрахункової палати Національного банку України в разі відмови в акредитації центру сертифікації ключів):

_____ (зазначити підставу для відмови в акредитації центру сертифікації ключів)

Рішення про відмову в акредитації № _____ від “_____” _____ року.

_____ (підпис)

_____ (прізвище, ім'я, по батькові начальника територіального управління/Центральної розрахункової палати Національного банку України)

_____ (підпис)

_____ (прізвище, ім'я, по батькові адміністратора реєстрації Засвідчувального центру Національного банку України)

“_____” _____ року

М. П.

Додаток 5
до Регламенту роботи Засвідчувального
центру Національного банку України
(пункт 6 розділу VI)

Заява про формування посиленого сертифіката
відкритого ключа центру сертифікації ключів
у Засвідчувальному центрі Національного банку України

Начальникові Управління Національного банку України
в/у _____ області (Центральної
розрахункової палати Національного банку України)

(прізвище, ім'я, по батькові)

(прізвище, ім'я, по батькові заявника)

_____ серія _____ № _____

(назва документа, що посвідчує особу заявника)

виданий “ _____ ” _____ року

(найменування органу, який видав документ, що посвідчує особу заявника)

що діє на підставі довіреності № _____

від “ _____ ” _____ року,

контактний телефон _____.

Прошу виконати процедуру формування посиленого сертифіката
відкритого ключа для центру сертифікації ключів відповідно до таких даних:

повне найменування центру сертифікації ключів:

_____ ;
_____ ;

дані, що вносяться до посиленого сертифіката відкритого ключа:

унікальний серійний номер центру сертифікації ключів: UA- _____ - _____,

область (S) _____ ;
 місто (L) _____ ;
 країна (C) UA _____ ;
 загальна назва (CN)¹ _____ ;
 підрозділ (OU)² _____ ;
 організація (O)³ _____ .

Посилений сертифікат відкритого ключа формується на такій основі⁴:
 запит на формування сертифіката _____ ;
 самопідписаний сертифікат _____ .

Значення серійного (заводського) номера носія інформації, на якому надається запит на формування сертифіката/самопідписаний сертифікат: _____ .

Розповсюдження посиленого сертифіката відкритого ключа центру сертифікації ключів, крім інформаційного ресурсу Засвідчувального центру Національного банку України, здійснювати:

засобами електронної пошти (e-mail) на адресі⁵:
 _____ ;

засобами електронної пошти Національного банку України на адресі⁵:
 _____ .

Розповсюдження списку відкликаних сертифікатів відкритих ключів, крім інформаційного ресурсу Засвідчувального центру Національного банку України, здійснювати:

засобами електронної пошти (e-mail) на адресі⁵:
 _____ ;

засобами електронної пошти Національного банку України на адресі⁵:
 _____ .

¹ Зазначається повне найменування центру сертифікації ключів.

² Зазначається “ЦСК” – для центру сертифікації ключів чи “АЦСК” – для акредитованого центру сертифікації ключів.

³ Зазначається повне найменування юридичної особи за установчими документами або відомостями про державну реєстрацію.

⁴ Зазначається назва файла.

⁵ Зазначається в разі необхідності.

(підпис)

(посада, прізвище, ім'я, по батькові керівника/заступника керівника центру сертифікації ключів)

“ _____ ” _____ року

М. П.

Заяву отримано, зареєстровано під № _____, особу заявника центру сертифікації ключів встановлено, відомості, зазначені в заяві, перевірено (заповнюється посадовими особами відповідного територіального управління/Центральної розрахункової палати Національного банку України).

Посилений сертифікат відкритого ключа центру сертифікації ключів сформовано. Серійний номер посиленого сертифіката (заповнюється посадовими особами відповідного територіального управління/Центральної розрахункової палати Національного банку України в разі формування посиленого сертифіката відкритого ключа): _____.

Центру сертифікації ключів відмовлено у формуванні посиленого сертифіката відкритого ключа на підставі (заповнюється посадовими особами відповідного територіального управління/Центральної розрахункової палати Національного банку України в разі відмови у формуванні посиленого сертифіката відкритого ключа):

(зазначити підставу відмови у формуванні посиленого сертифіката відкритого ключа)

(підпис)

(прізвище, ім'я, по батькові начальника територіального управління/Центральної розрахункової палати Національного банку України)

(підпис)

(прізвище, ім'я, по батькові адміністратора реєстрації Засвідчувального центру Національного банку України)

“ _____ ” _____ року

М. П.

Додаток 6
до Регламенту роботи Засвідчувального
центру Національного банку України
(пункт 6 розділу VI)

Заява про внесення змін до реєстраційних даних
zareєстрованого/акредитованого центру сертифікації ключів
у Засвідчувальному центрі Національного банку України

Начальникові Управління Національного банку України
в/у _____ області (Центральної
розрахункової палати Національного банку України)

(прізвище, ім'я, по батькові)

(прізвище, ім'я, по батькові заявника)

_____ серія _____ № _____

(назва документа, що посвідчує особу заявника)

виданий “ _____ ” _____ року

(найменування органу, який видав документ, що посвідчує особу заявника)

що діє на підставі довіреності № _____

від “ _____ ” _____ року,

контактний телефон _____.

У зв'язку зі зміною ідентифікаційних даних центру сертифікації ключів

(повне найменування центру сертифікації ключів згідно з ідентифікаційними даними,

унесеними до реєстру Засвідчувального центру Національного банку України)

(свідоцтво про реєстрацію/акредитацію, серія _____ № _____

від “ _____ ” _____ року) прошу внести такі ідентифікаційні
дані до реєстру Засвідчувального центру Національного банку України,
зазначені в заяві:

повне найменування юридичної особи:

_____ ;

повне найменування центру сертифікації ключів:

_____ ;

унікальний серійний номер центру сертифікації ключів¹: UA- _____ - ____ ;

ідентифікаційний код юридичної особи за ЄДРПОУ _____ ;

організаційно-правова форма _____ ;

місцезнаходження центру сертифікації ключів:

поштовий індекс _____ ;

область _____ ;

район області _____ ;

населений пункт _____ ;

вулиця _____ ;

будинок _____, корпус _____, офіс _____ ;

телефон _____ ;

факс _____ ;

електронна пошта _____ ;

електронна адреса інформаційного ресурсу _____ .

¹ Значення цього реквізиту має такий вигляд:

UA-[код установи]{-[додаток]},

де код установи – ідентифікаційний код юридичної особи за ЄДРПОУ;

додаток – необов'язкова послідовність від 1 до 4 цифр, що містить додаткову частину ідентифікатора.

До заяви додаються:

_____ (перелік документів, які додаються до заяви про реєстрацію/акредитацію

_____ центру сертифікації ключів, що зазнали змін унаслідок зміни реєстраційних даних)

_____ (підпис)

_____ (посада, прізвище, ім'я, по батькові керівника/заступника керівника центру сертифікації ключів)

“ _____ ” _____ року

М. П.

Заяву отримано, зареєстровано під № _____, особу заявника Центру сертифікації ключів встановлено, відомості, зазначені в заяві, перевірено (заповнюється посадовими особами відповідного територіального управління/Центральної розрахункової палати Національного банку України).

Реєстраційні дані, зазначені в заяві, унесено до реєстру Засвідчувального центру Національного банку України, центру сертифікації ключів присвоєно унікальний серійний номер UA-_____ - _____ (заповнюється посадовими особами відповідного територіального управління/Центральної розрахункової палати Національного банку України).

Центру сертифікації ключів відмовлено у внесенні змінених ідентифікаційних даних до реєстру Засвідчувального центру Національного банку України на підставі (заповнюється посадовими особами відповідного територіального управління/Центральної розрахункової палати Національного банку України в разі відмови у внесенні змінених ідентифікаційних даних центру сертифікації ключів):

_____ (зазначити підставу відмови у внесенні змінених ідентифікаційних даних центру сертифікації ключів)

_____.

Рішення про відмову у внесенні змінених ідентифікаційних даних центру сертифікації ключів: № _____ від “ _____ ” _____ року.

_____ (підпис)

_____ (прізвище, ім'я, по батькові начальника територіального управління/Центральної розрахункової палати Національного банку України)

_____ (підпис)

_____ (прізвище, ім'я, по батькові адміністратора реєстрації Засвідчувального центру Національного банку України)

“ _____ ” _____ року

М. П.

Додаток 7
до Регламенту роботи Засвідчувального
центру Національного банку України
(пункт 6 розділу VI)

Заява про видачу дубліката свідоцтва
про реєстрацію/акредитацію центру сертифікації ключів
у Засвідчувальному центрі Національного банку України

Начальникові Управління Національного банку України
в/у _____ області (Центральної
розрахункової палати Національного банку України)

_____ (прізвище, ім'я, по батькові)

_____ (прізвище, ім'я, по батькові заявника)

_____ серія _____ № _____
(назва документа, що посвідчує особу заявника)

виданий “ _____ ” _____ року

_____ (найменування органу, який видав документ, що посвідчує особу заявника)

що діє на підставі довіреності № _____

від “ _____ ” _____ року,

контактний телефон _____.

У зв'язку із втратою/пошкодженням свідоцтва про реєстрацію/акредитацію
центру сертифікації ключів

_____ (повне найменування центру сертифікації ключів згідно з ідентифікаційними даними,

унесеними до реєстру Засвідчувального центру Національного банку України)

(свідоцтво про реєстрацію/акредитацію, серія _____ № _____

від “ _____ ” _____ року) прошу видати дублікат свідоцтва
про реєстрацію/акредитацію центру сертифікації ключів у Засвідчувальному
центрі Національного банку України.

(підпис) _____
(посада, прізвище, ім'я, по батькові керівника/заступника керівника
центру сертифікації ключів)

“ _____ ” _____ року

М. П.

Заяву отримано, зареєстровано під № _____, особу заявника центру сертифікації ключів встановлено, відомості, зазначені в заяві, перевірено (заповнюється посадовими особами відповідного територіального управління/Центральної розрахункової палати Національного банку України).

Дублікат свідоцтва про реєстрацію/акредитацію видано.

(підпис) _____
(прізвище, ім'я, по батькові начальника територіального управління/Центральної
розрахункової палати Національного банку України)

(підпис) _____
(прізвище, ім'я, по батькові адміністратора реєстрації Засвідчувального центру
Національного банку України)

“ _____ ” _____ року

М. П.

Додаток 8
до Регламенту роботи Засвідчувального
центру Національного банку України
(пункт 6 розділу VI)

Свідоцтво
про реєстрацію/акредитацію центру сертифікації ключів
у Засвідчувальному центрі Національного банку України

Серія _____ № _____

Згідно з рішенням Засвідчувального центру Національного банку України
від “ _____ ” _____ року № _____,
на підставі заяви центру сертифікації ключів про реєстрацію/акредитацію
від “ _____ ” _____ року № _____

(повне найменування центру сертифікації ключів)

UA-

(унікальний серійний номер центру сертифікації ключів)

(повне найменування юридичної особи)

(ідентифікаційний код за ЄДРПОУ)

відповідає вимогам до зареєстрованого/акредитованого центру сертифікації
ключів і внесений “ _____ ” _____ року до реєстру Засвідчувального
центру Національного банку України.

Місцезнаходження зареєстрованого/акредитованого центру сертифікації ключів:

поштовий індекс _____ ;

область _____ ;

район області _____ ;

населений пункт _____ ;

вулиця _____ ;

будинок _____, корпус _____, офіс _____ ;

телефон _____ ;

факс _____ ;

Свідоцтво дійсне до¹ “ _____ ” _____ року.

(підпис)

(прізвище, ім'я, по батькові начальника територіального управління/Центральної розрахункової палати Національного банку України)

(підпис)

(прізвище, ім'я, по батькові адміністратора реєстрації Засвідчувального центру Національного банку України)

“ _____ ” _____ року

М. П.

¹ Зазначається для акредитованого центру сертифікації ключів.

Додаток 9
до Регламенту роботи Засвідчувального
центру Національного банку України
(пункт 8 розділу IX)

Дозвіл суб'єктів персональних даних на обробку їх персональних даних
у Засвідчувальному центрі Національного банку України

Ми, що нижче підписалися, надаємо дозвіл на обробку наших
персональних даних, які передаються до Засвідчувального центру
Національного банку України для проведення _____

_____ (назва регламентної процедури)

_____ (повне найменування центру сертифікації ключів)

унікальний серійний номер центру сертифікації ключів: UA- _____ - _____.

(підпис)

(посада, прізвище, ім'я, по батькові керівника/
заступника керівника центру сертифікації ключів)

(підпис)

(посада, прізвище, ім'я, по батькові заявника
центру сертифікації ключів)

(підпис)

(посада, прізвище, ім'я, по батькові відповідальної особи
центру сертифікації ключів)

“ _____ ” _____ року

М. П.