

ПОРІВНЯЛЬНА ТАБЛИЦЯ

<p style="text-align: center;">Постанова Кабінету Міністрів України від 13 липня 2004 року № 903 «Про затвердження Порядку акредитації центру сертифікації ключів»</p>	<p style="text-align: center;">Закон України «Про електронні довірчі послуги»</p>
<p>1. Цей Порядок визначає процедуру акредитації центру сертифікації ключів (далі - центр), умови надання центром послуг електронного цифрового підпису, вимоги до його персоналу та захисту інформації.</p>	
<p>2. Терміни, які вживаються у цьому Порядку, мають таке значення:</p> <p style="padding-left: 40px;">контролюючий орган - Адміністрація Держспецзв'язку;</p> <p style="padding-left: 40px;">програмно-технічний комплекс - апаратні, апаратно-програмні та програмні засоби акредитованого центру, що забезпечують виконання функцій, пов'язаних з наданням послуг електронного цифрового підпису;</p> <p style="padding-left: 40px;">спеціальне приміщення - приміщення, яке відповідає вимогам технічного захисту інформації;</p> <p style="padding-left: 40px;">правила посиленої сертифікації - затверджені в установленому порядку вимоги до обслуговування та використання посилених сертифікатів відкритих ключів (далі - сертифікати);</p> <p style="padding-left: 40px;">регламент роботи акредитованого центру - нормативний документ, що визначає організаційні, технічні та інші умови</p>	<p style="text-align: center;">Стаття 8 частина 1</p> <p style="padding-left: 40px;">Спеціально уповноважений центральний орган виконавчої влади з питань організації спеціального зв'язку та захисту інформації виконує функції контролюючого органу у сфері електронних довірчих послуг.</p> <p style="text-align: center;">Стаття 1. Визначення термінів</p> <p style="padding-left: 40px;">34) програмно-технічний комплекс, що використовується під час надання електронних довірчих послуг (далі - програмно-технічний комплекс), - апаратні, апаратно-програмні та програмні засоби, що забезпечують виконання функцій, пов'язаних з наданням електронних довірчих послуг;</p>

діяльності акредитованого центру під час надання послуг електронного цифрового підпису;

список відкликаних сертифікатів - перелік блокованих та скасованих сертифікатів, що формується та розповсюджується акредитованим центром;

статус сертифіката - стан посиленого сертифіката ключа (чинний, блокований, скасований) на конкретний момент.

Інші терміни застосовуються у значенні, наведеному у Законах України "Про електронний цифровий підпис", "Про телекомунікації", інших нормативно-правових актах з питань інформатизації та захисту інформації.

35) реєстр чинних, блокованих та скасованих сертифікатів відкритих ключів - електронна база даних, в якій містяться відомості про сертифікати відкритих ключів, сформовані надавачем електронних довірчих послуг, засвідчувальним центром або центральним засвідчувальним органом, їх статус та списки відкликаних сертифікатів відкритих ключів;

6) Довірчий список - перелік кваліфікованих надавачів електронних довірчих послуг та інформації про послуги, що ними надаються;

7) електронна довірча послуга - послуга, яка надається для забезпечення електронної взаємодії двох або більше суб'єктів, які довіряють надавачу електронних довірчих послуг щодо надання такої послуги;

24) кваліфікований надавач електронних довірчих послуг - юридична особа незалежно від організаційно-правової форми та форми власності, фізична особа - підприємець, яка надає одну або більше електронних довірчих послуг, діяльність якої відповідає вимогам цього Закону та відомості про яку внесені до Довірчого списку;

28) надавач електронних довірчих послуг - юридична особа незалежно від організаційно-правової форми та форми

	власності, фізична особа - підприємець, яка надає одну або більше електронних довірчих послуг; Закон України «Про електронні довірчі послуги»
3. Акредитація центру здійснюється на добровільних засадах.	_____
4. Інформація про акредитацію центру сертифікації ключів та припинення його діяльності оприлюднюється центральним засвідчувальним органом на власному веб-сайті.	<p>Стаття 35 Довірчий список</p> <p>1. Центральний засвідчувальний орган впроваджує, підтримує в актуальному стані та публікує на своєму офіційному веб-сайті Довірчий список, в якому міститься інформація про кваліфікованих надавачів електронних довірчих послуг разом з інформацією про кваліфіковані електронні довірчі послуги, які вони надають.</p> <p>Довірчий список повинен впроваджуватися, підтримуватися в актуальному стані та публікуватися в безпечному режимі з обов'язковим додаванням електронної печатки центрального засвідчувального органу у вигляді, придатному для автоматичної обробки.</p> <p>Інформація, що міститься у Довірчому списку, є відкритою.</p>
5. До проведення акредитації центр вносить на спеціальний рахунок, відкритий у банківській установі, кошти у розмірі стократною мінімальною заробітної плати для забезпечення відшкодування збитків, які можуть бути завдані підписувачам, користувачам або третім особам внаслідок неналежного виконання акредитованим центром своїх зобов'язань.	<p>Стаття 16. Вимоги до електронних довірчих послуг</p> <p>3. Діяльність кваліфікованих надавачів електронних довірчих послуг здійснюється за умови внесення коштів на поточний рахунок із спеціальним режимом використання у банку (рахунок в органі, що здійснює казначейське обслуговування бюджетних коштів) або страхування цивільно-правової відповідальності для забезпечення відшкодування шкоди, яка може бути завдана користувачам таких послуг чи третім особам. Розмір внеску на поточному</p>
Наявність спеціального рахунка не обов'язкова для акредитованого центру, який надає пов'язані з електронним	

<p><i>цифровим підписом послуги виключно органам державної влади.</i></p>	<p>рахунку із спеціальним режимом використання у банку (рахунку в органі, що здійснює казначейське обслуговування бюджетних коштів) або страхової суми не може становити менш як 1000 мінімальних розмірів заробітної плати.</p>
<p>6. Для проведення акредитації центр, що засвідчив свій відкритий ключ у центральному засвідчувальному органі та вніс кошти на спеціальний рахунок, подає до нього заяву разом із документами, перелік яких наведено у додатку 1.</p> <p>У заяві зазначаються:</p> <p>повне найменування юридичної особи, посада, прізвище, ім'я та по батькові її керівника (прізвище, ім'я та по батькові фізичної особи - суб'єкта підприємницької діяльності, серія і номер паспорта, ким і коли виданий);</p> <p>організаційно-правова форма;</p> <p>код згідно з ЄДРПОУ (реєстраційний номер облікової картки платника податків (ідентифікаційний номер);</p> <p>номер поточного рахунка та найменування банківської установи;</p> <p>місцезнаходження (місце проживання);</p> <p>номери телефонів;</p> <p>електронна адреса електронного інформаційного ресурсу;</p> <p>відомості про реєстрацію відкритого ключа в центральному засвідчувальному органі.</p>	<p>Стаття 30. Набуття статусу кваліфікованого надавача електронних довірчих послуг</p> <p>2. Юридичні особи, фізичні особи - підприємці для внесення відомостей про них до Довірчого списку подають до центрального засвідчувального органу або засвідчувального центру:</p> <ol style="list-style-type: none"> 1) заяву про внесення до Довірчого списку; 2) документ, що дає змогу однозначно ідентифікувати фізичну особу - підприємця або представника юридичної особи; 3) засвідчену в установленому законодавством порядку копію атестата відповідності комплексної системи захисту інформації вимогам нормативних документів у сфері захисту інформації із засвідченою в установленому законодавством порядку копією позитивного експертного висновку за результатами державної експертизи у сфері криптографічного захисту інформації або засвідчену в установленому законодавством порядку копію документа про відповідність, складеного за результатами проведення процедури оцінки відповідності у сфері електронних довірчих послуг; 4) засвідчені в установленому законодавством порядку копії документів, які підтверджують право власності або право користування нежилими приміщеннями, які

Додаток 1
до Порядку

Перелік документів, що подаються разом із заявою про акредитацію

1. Копії установчих документів, засвідчені в установленому порядку (для юридичної особи).
4. Копії паспорта, довіреності або іншого документа, що підтверджують повноваження фізичної особи на представлення інтересів суб'єкта підприємницької діяльності.
5. Копія документа, що підтверджує право власності центру сертифікації ключів на окреме приміщення або оренду такого приміщення, засвідчена в установленому порядку.
6. Копія документа про внесення на спеціальний рахунок коштів для забезпечення відшкодування збитків, які можуть бути завдані акредитованим центром підписувачам, користувачам або третім особам внаслідок неналежного виконання своїх зобов'язань.
7. Документ, що підтверджує внесення плати за проведення акредитації.
8. Копія атестата відповідності комплексної системи захисту інформації вимогам нормативних документів у сфері захисту інформації.
9. Копії сертифікатів відповідності або позитивних

використовуватимуться для розміщення всіх складових програмно-технічного комплексу, що забезпечуватимуть надання кваліфікованих електронних довірчих послуг;

5) персональний та посадовий склад працівників, обов'язки яких будуть безпосередньо пов'язані з наданням кваліфікованих електронних довірчих послуг;

6) засвідчені в установленому законодавством порядку копії документів, які підтверджують освітньо-кваліфікаційний рівень та трирічний стаж роботи за фахом найманих працівників, обов'язки яких будуть безпосередньо пов'язані з наданням кваліфікованих електронних довірчих послуг;

7) засвідчені в установленому законодавством порядку копії документів, які підтверджують право власності або право користування засобами кваліфікованого електронного підпису чи печатки, які використовуватимуться для надання кваліфікованих електронних довірчих послуг;

8) засвідчену в установленому законодавством порядку копію договору страхування цивільно-правової відповідальності або засвідчені в установленому законодавством порядку копії документів, що підтверджують внесення коштів на поточний рахунок із спеціальним режимом використання у банку (рахунок в органі, що здійснює казначейське обслуговування бюджетних коштів) для забезпечення відшкодування збитків, які можуть бути заподіяні кваліфікованим надавачем електронних довірчих послуг користувачам електронних довірчих послуг унаслідок неналежного виконання своїх обов'язків;

експертних висновків за результатами державної експертизи у сфері криптографічного захисту інформації.

10. Список посадових осіб центру сертифікації ключів та засвідчені в установленому порядку копії документів про рівень освіти і кваліфікації керівника центру сертифікації ключів та посадових осіб, обов'язки яких безпосередньо пов'язані з наданням послуг електронного цифрового підпису та обслуговуванням посилених сертифікатів відкритих ключів.

11. Регламент роботи центру сертифікації ключів, затверджений керівником та погоджений контролюючим органом.

12. Положення, яким визначаються посадові обов'язки, кваліфікаційні вимоги та відповідальність посадових осіб центру сертифікації ключів.

13. Положення про службу захисту інформації центру сертифікації ключів, затверджене його керівником.

14. План-схема приміщень центру сертифікації ключів та порядок доступу до спеціальних приміщень.

15. Порядок зберігання окремих резервних копій посилених сертифікатів ключів та списків відкликаних сертифікатів, сформованих акредитованим центром.

16. Порядок синхронізації з Всесвітнім координованим часом (UTC).

17. Відомості про ліцензії на право провадження

9) засвідчену в установленому законодавством порядку копію регламенту роботи кваліфікованого надавача електронних довірчих послуг, погодженого з контролюючим органом (або засвідчувальним центром - для надавачів електронних довірчих послуг, що вносяться до Довірчого списку за поданням засвідчувального центру), що відповідає вимогам до регламенту кваліфікованого надавача електронних довірчих послуг;

10) копії документів, передбачених пунктами 1-9 цієї частини, в електронній формі.

У разі надання електронних довірчих послуг у банківській системі України та при здійсненні переказу коштів відомості до Довірчого списку вносяться за поданням засвідчувального центру.

<p>господарської діяльності в галузі криптографічного або технічного захисту інформації (у разі наявності).</p> <p>18. Довіреність особи для представництва інтересів центру перед центральним засвідчувальним органом.</p>	
<p>7. На підставі заяви та доданих до неї документів центральний засвідчувальний орган у строк не більше ніж 45 днів від дати подання заяви приймає рішення про акредитацію центру або про відмову в акредитації.</p> <p>У разі необхідності центральний засвідчувальний орган здійснює перевірку центру на відповідність вимогам цього Порядку.</p>	<p>Стаття 30. Набуття статусу кваліфікованого надавача електронних довірчих послуг</p> <p>4. Центральний засвідчувальний орган або засвідчувальний центр за результатами розгляду поданих документів протягом 15 робочих днів з дня реєстрації заяви про внесення до Довірчого списку приймає рішення про внесення кваліфікованого надавача електронних довірчих послуг або надсилає вмотивовану відмову у внесенні відомостей до Довірчого списку.</p> <p>6. Центральний засвідчувальний орган або засвідчувальний центр приймає рішення про відмову у внесенні відомостей до Довірчого списку в разі:</p> <p>подання не в повному обсязі документів, передбачених частиною другою цієї статті;</p> <p>виявлення в заяві про внесення до Довірчого списку та документах, що додаються до неї, недостовірної інформації, пошкоджень, які не дають змоги однозначно тлумачити зміст, виправлень або дописок.</p>
<p>8. Центр вважається акредитованим від дня внесення до Реєстру суб'єктів, які надають послуги, пов'язані з електронним цифровим підписом (далі - Реєстр), що ведеться центральним засвідчувальним органом, основних даних (реквізитів) акредитованого центру, зазначених у</p>	<p>Стаття 30. Набуття статусу кваліфікованого надавача електронних довірчих послуг</p> <p>1. Статусу кваліфікованого надавача електронних довірчих послуг юридичні особи, фізичні особи - підприємці</p>

<p>пункті 6 цього Порядку, відомостей про дату прийняття та номер рішення про акредитацію, серію та номер свідоцтва, а також строк дії свідоцтва.</p>	<p>набувають з дня внесення відомостей про них до Довірчого списку на підставі рішення центрального засвідчувального органу або засвідчувального центру (у разі надання електронних довірчих послуг у банківській системі України та при здійсненні переказу коштів).</p> <p>5. Кваліфікований надавач електронних довірчих послуг на підставі прийнятого центральним засвідчувальним органом або засвідчувальним центром рішення про внесення відомостей про нього до Довірчого списку засвідчує свій відкритий ключ у центральному засвідчувальному органі або засвідчувальному центрі відповідно до вимог регламенту роботи центрального засвідчувального органу або засвідчувального центру.</p>
<p>9. У разі прийняття центральним засвідчувальним органом рішення про акредитацію, центрові видається свідоцтво про акредитацію (далі - свідоцтво) за зразком, наведеним у додатку 2.</p> <p>Копії рішення про акредитацію та свідоцтва надсилаються до контролюючого органу.</p>	<p>_____</p>
<p>10. Свідоцтво видається уповноваженому представнику центру протягом п'яти робочих днів від дати внесення відповідного запису до Реєстру.</p>	<p>_____</p>
<p>11. У разі зміни відомостей, які внесені до Реєстру, акредитований центр у триденний строк повідомляє про це центральний засвідчувальний орган.</p>	<p>Стаття 30. Набуття статусу кваліфікованого надавача електронних довірчих послуг</p> <p>7. Зміна відомостей про кваліфікованого надавача електронних довірчих послуг, що містяться в Довірчому списку, є підставою для внесення змін до Довірчого списку.</p> <p>Кваліфікований надавач електронних довірчих послуг у</p>

	<p>разі виникнення підстав для внесення змін до Довірчого списку зобов'язаний протягом п'яти робочих днів з дня настання таких підстав подати до органу, який приймав рішення про внесення відомостей про нього до Довірчого списку, заяву про внесення змін до Довірчого списку разом з документами, що підтверджують відповідні зміни.</p> <p>Центральний засвідчувальний орган протягом п'яти календарних днів з дня реєстрації заяви про внесення змін до Довірчого списку зобов'язаний внести відповідні зміни до Довірчого списку або надати вмотивовану відмову у внесенні до Довірчого списку.</p>
<p>12. У разі пошкодження або втрати свідоцтва центрові видається протягом десяти днів від дати подання відповідної заяви його дублікат.</p> <p>Відомості про видачу дубліката вносяться до Реєстру.</p>	<p>_____</p>
<p>13. Акредитований центр проходить повторну акредитацію у разі:</p> <p><i>зміни основних даних (реквізитів), які зазначаються у свідоцтві;</i></p> <p><i>закінчення строку дії свідоцтва;</i></p> <p><i>закінчення строку дії атестата відповідності комплексної системи захисту інформації чи втрати чинності таким атестатом або модернізації програмно-технічного комплексу акредитованого центру;</i></p> <p><i>закінчення строку дії сертифіката відповідності або позитивного експертного висновку, за результатами державної експертизи у сфері криптографічного захисту інформації;</i></p>	

<p><i>повідомлення контролюючим органом щодо порушення порядку проведення акредитації.</i></p> <p><i>Повторна акредитація здійснюється згідно з пунктами 5 - 10 цього Порядку.</i></p>	
<p>14. Рішення про скасування акредитації центральний засвідчувальний орган приймає у разі:</p> <p>повідомлення контролюючим органом про порушення акредитованим центром законодавства;</p> <p>неукладення протягом року жодного договору про надання послуг електронного цифрового підпису;</p> <p>непоповнення спеціального рахунка для забезпечення відшкодування збитків;</p> <p>невиконання акредитованим центром встановлених вимог щодо надання послуг електронного цифрового підпису згідно із законодавством;</p> <p>прийняття акредитованим центром рішення про припинення діяльності.</p> <p>Про прийняте рішення центральний засвідчувальний орган в односторонній строк повідомляє акредитованому центру, а також розміщує відповідну інформацію на власному веб-сайті.</p>	<p>Стаття 30. Набуття статусу кваліфікованого надавача електронних довірчих послуг</p> <p>9. Центральний засвідчувальний орган приймає рішення про виключення кваліфікованого надавача електронних довірчих послуг з Довірчого списку в разі отримання:</p> <p>заяви кваліфікованого надавача електронних довірчих послуг про виключення відомостей про нього з Довірчого списку;</p> <p>подання засвідчувального центру про виключення кваліфікованого надавача електронних довірчих послуг з Довірчого списку;</p> <p>подання контролюючого органу про виключення кваліфікованого надавача електронних довірчих послуг з Довірчого списку за результатами перевірки дотримання вимог законодавства у сфері електронних довірчих послуг;</p> <p>інформації про припинення діяльності кваліфікованого надавача електронних довірчих послуг (державної реєстрації припинення підприємницької діяльності фізичної особи - підприємця чи припинення діяльності в установленому законодавством порядку юридичної особи);</p>

	<p>інформації про смерть кваліфікованого надавача електронних довірчих послуг (фізичної особи - підприємця);</p> <p>інформації про набрання законної сили рішенням суду про виключення кваліфікованого надавача електронних довірчих послуг з Довірчого списку, оголошення кваліфікованого надавача електронних довірчих послуг померлим, визнання його безвісно відсутнім, недієздатним, обмеження його цивільної дієздатності, визнання кваліфікованого надавача електронних довірчих послуг банкрутом.</p>
<p>15. У разі прийняття рішення про скасування акредитації свідоцтво анулюється.</p>	<p>Стаття 31. Припинення діяльності з надання кваліфікованих електронних довірчих послуг кваліфікованим надавачем електронних довірчих послуг</p> <p>1. Кваліфікований надавач електронних довірчих послуг припиняє свою діяльність з надання кваліфікованих електронних довірчих послуг у разі:</p> <p>прийняття центральним засвідчувальним органом рішення про виключення його з Довірчого списку;</p> <p>прийняття ним рішення про припинення надання кваліфікованих електронних довірчих послуг, що зазначені у Довірчому списку;</p> <p>припинення діяльності кваліфікованого надавача електронних довірчих послуг (державної реєстрації припинення підприємницької діяльності фізичної особи - підприємця чи припинення діяльності в установленому законодавством порядку юридичної особи);</p> <p>набрання законної сили рішенням суду про виключення</p>

його з Довірчого списку, оголошення його померлим, визнання безвісно відсутнім, недієздатним, обмеження його цивільної дієздатності, визнання його банкрутом.

2. Про прийняття рішення про припинення надання кваліфікованих електронних довірчих послуг кваліфікований надавач електронних довірчих послуг зобов'язаний повідомити користувачам електронних довірчих послуг, центральному засвідчувальному органу або засвідчувальному центру та контролюючому органу не пізніше ніж через п'ять робочих днів з дня прийняття такого рішення.

3. Центральний засвідчувальний орган та/або засвідчувальний центр зобов'язаний оприлюднити інформацію про рішення відповідно центрального засвідчувального органу або засвідчувального центру щодо припинення кваліфікованим надавачем електронних довірчих послуг надання кваліфікованих електронних довірчих послуг чи виключення кваліфікованого надавача електронних довірчих послуг центральним засвідчувальним органом з Довірчого списку не пізніше ніж протягом наступного робочого дня після прийняття такого рішення шляхом:

розміщення інформації про це рішення на своєму офіційному веб-сайті;

надіслання кваліфікованому надавачу електронних довірчих послуг повідомлення про це рішення із зазначенням підстав для скасування.

	<p>5. Кваліфікований надавач електронних довірчих послуг припиняє свою діяльність з надання кваліфікованих електронних довірчих послуг через три місяці з дня опублікування відповідно центральним засвідчувальним органом або засвідчувальним центром на своєму офіційному веб-сайті повідомлення про припинення надання кваліфікованих електронних довірчих послуг кваліфікованим надавачем електронних довірчих послуг.</p>
<p>16. Відомості про скасування акредитації та анулювання свідоцтва центральний засвідчувальний орган вносить до Реєстру після передачі акредитованим центром документованої інформації на зберігання центральному засвідчувальному органу і повідомляє про це акредитований центр та контролюючий орган із зазначенням підстав скасування акредитації.</p>	<p>Стаття 31. Припинення діяльності з надання кваліфікованих електронних довірчих послуг кваліфікованим надавачем електронних довірчих послуг</p> <p>4. Центральний засвідчувальний орган та/або засвідчувальний центр зобов'язаний опублікувати на своєму офіційному веб-сайті повідомлення про припинення надання кваліфікованих електронних довірчих послуг кваліфікованим надавачем електронних довірчих послуг не пізніше ніж протягом наступного робочого дня з дня одержання повідомлення про настання підстав, передбачених абзацами третім - п'ятим частини першої цієї статті.</p> <p>Повідомлення центрального засвідчувального органу або засвідчувального центру про припинення надання кваліфікованих електронних довірчих послуг кваліфікованим надавачем електронних довірчих послуг повинно містити дату опублікування.</p>
<p>17. Центр, якому було відмовлено в акредитації у зв'язку з поданням недостовірної інформації або акредитацію якого було скасовано, не може бути акредитований протягом року від дати прийняття рішення про відмову в акредитації або про скасування акредитації.</p>	<p>_____</p>
<p>18. Рішення про відмову в акредитації або скасування</p>	<p>_____</p>

<p><i>акредитації може бути оскаржено в судовому порядку.</i></p>	
<p>19. За проведення акредитації справляється плата у розмірі, встановленому Кабінетом Міністрів України.</p>	<p>Стаття 29. Особливості надання кваліфікованих електронних довірчих послуг центральним засвідчувальним органом</p> <p>2. Договір про надання центральним засвідчувальним органом кваліфікованої електронної довірчої послуги формування, перевірки та підтвердження чинності кваліфікованого сертифіката електронного підпису чи печатки повинен містити умови щодо:</p> <p>Центральний засвідчувальний орган надає кваліфіковану електронну довірчу послугу формування, перевірки та підтвердження чинності кваліфікованого сертифіката електронного підпису чи печатки безоплатно для органів державної влади, місцевого самоврядування, інших юридичних осіб публічного права.</p>
<p>20. Акредитований центр:</p> <p>забезпечує виконання вимог щодо надання послуг електронного цифрового підпису згідно із законом;</p> <p>інформує підписувача про обмеження використання електронного цифрового підпису та порядок відшкодування збитків;</p> <p>виконує приписи контролюючого органу;</p> <p>надає допомогу підписувачам під час генерації особистих та відкритих ключів у разі отримання від них відповідного звернення та вживає заходів щодо забезпечення безпеки інформації під час генерації;</p>	<p>Стаття 13. Права та обов'язки кваліфікованих надавачів електронних довірчих послуг</p> <p>1. Кваліфіковані надавачі електронних довірчих послуг мають право:</p> <p>надавати електронні довірчі послуги з дотриманням вимог цього Закону;</p> <p>отримувати документи, необхідні для ідентифікації особи, ідентифікаційні дані якої міститимуться у сертифікаті відкритого ключа;</p> <p>отримувати консультації від центрального засвідчувального органу або засвідчувального центру з питань, пов'язаних з наданням електронних довірчих</p>

<p>забезпечує розташування засобів програмно-технічного комплексу, за допомогою яких здійснюється надання послуг сертифікації та відкликання, в спеціальних приміщеннях та їх охорону;</p> <p>забезпечує збереження програмно-технічного комплексу, іншого майна та запобігання безконтрольному проникненню в приміщення акредитованого центру сторонніх осіб;</p> <p>використовує надійні засоби електронного цифрового підпису, програмно-технічний комплекс, засоби криптографічного захисту інформації відповідно до вимог Адміністрації Державної служби спеціального зв'язку та захисту інформації і Мін'юсту.</p>	<p>послуг;</p> <p>звертатися до органів з оцінки відповідності для отримання документів про відповідність;</p> <p>звертатися із заявою про скасування, блокування або поновлення сформованих у центральному засвідчувальному органі або засвідчувальному центрі кваліфікованих сертифікатів відкритих ключів;</p> <p>самостійно обирати, які саме стандарти будуть ними застосовуватися при наданні довірчих послуг з переліку стандартів, визначеного Кабінетом Міністрів України, крім сфери спеціального зв'язку.</p>
<p><i>21. Надання послуг електронного цифрового підпису здійснюється акредитованим центром згідно з правилами посиленої сертифікації та регламентом роботи цього центру.</i></p>	<p>_____</p>
<p>22. Акредитований центр під час надання послуг електронного цифрового підпису фізичним та юридичним особам, фізичним особам - підприємцям зобов'язаний дотримуватися таких вимог:</p> <p>встановлювати відповідно до законодавства фізичну особу, фізичну особу - підприємця, юридичну особу та уповноваженого представника юридичної особи, які звернулися до акредитованого центру з метою формування сертифіката;</p> <p>перевіряти дані, обов'язкові для формування сертифіката, і дані, які вносяться до нього на вимогу підписувача;</p>	<p>Стаття 13. Права та обов'язки кваліфікованих надавачів електронних довірчих послуг</p> <p>2. Кваліфіковані надавачі електронних довірчих послуг зобов'язані забезпечити:</p> <p>захист персональних даних користувачів електронних довірчих послуг відповідно до вимог законодавства;</p> <p>функціонування програмно-технічного комплексу, що ними використовується, та захист інформації, що в ньому обробляється, відповідно до вимог законодавства;</p> <p>створення та функціонування свого веб-сайту;</p>

реєструвати та вести облік звернень фізичних та юридичних осіб, на підставі яких були сформовані сертифікати;

встановлювати належність підписувачу особистого ключа та його відповідність відкритому ключу, якщо їх генерація здійснювалася не в акредитованому центрі.

впровадження, підтримання в актуальному стані та публікацію на своєму веб-сайті реєстру чинних, блокованих та скасованих сертифікатів відкритих ключів;

можливість цілодобового доступу до реєстру чинних, блокованих та скасованих сертифікатів відкритих ключів та до інформації про статус сертифікатів відкритих ключів через телекомунікаційні мережі загального користування;

цілодобовий прийом та перевірку заяв підписувачів та створювачів електронних печаток про скасування, блокування та поновлення їхніх сертифікатів відкритих ключів;

скасування, блокування та поновлення сертифікатів відкритих ключів відповідно до вимог цього Закону;

встановлення під час формування сертифіката відкритого ключа належності відкритого ключа та відповідного йому особистого ключа підписувачу чи створювачу електронної печатки;

внесення ідентифікаційних даних підписувача чи створювача електронної печатки до відповідного сертифіката відкритого ключа;

інформування контролюючого органу про порушення конфіденційності та/або цілісності інформації, що впливають на надання електронних довірчих послуг або стосуються персональних даних користувачів електронних довірчих послуг, не пізніше 24 годин з моменту, коли їм стало відомо про таке порушення;

інформування користувачів електронних довірчих послуг про порушення конфіденційності та/або цілісності інформації, що впливають на надання їм електронних довірчих послуг або стосуються їхніх персональних даних, не пізніше двох годин з моменту, коли їм стало відомо про такі порушення;

унеможливлення використання особистого ключа у разі його компрометації;

постійне зберігання всіх виданих кваліфікованих сертифікатів відкритих ключів;

внесення коштів на поточний рахунок із спеціальним режимом використання у банку (рахунок в органі, що здійснює казначейське обслуговування бюджетних коштів) або страхування цивільно-правової відповідальності для забезпечення відшкодування шкоди, яка може бути заподіяна користувачам таких послуг чи третім особам внаслідок неналежного виконання кваліфікованим надавачем електронних довірчих послуг своїх зобов'язань, у розмірі, визначеному частиною третьою статті 16 цього Закону;

наймання працівників, які володіють необхідними для надання кваліфікованих електронних довірчих послуг знаннями, досвідом і кваліфікацією, у тому числі у сферах інформаційних технологій та захисту інформації;

використання під час надання електронних довірчих послуг виключно кваліфікованих сертифікатів, засвідчених у центральному засвідчувальному органі чи засвідчувальному центрі;

	<p>зберігання документів, поданих користувачами для отримання електронних довірчих послуг;</p> <p>інформування контролюючого органу та центрального засвідчувального органу або засвідчувального центру про будь-які зміни у процедурі надання електронних довірчих послуг протягом 48 годин з моменту настання таких змін;</p> <p>передачу центральному засвідчувальному органу або засвідчувальному центру документованої інформації в разі припинення діяльності з надання електронних довірчих послуг.</p>
<p>23. У разі використання коштів із спеціального рахунка для відшкодування завданих збитків акредитований центр зобов'язаний протягом 30 днів від дати здійснення такого відшкодування поповнити спеціальний рахунок до встановленого розміру.</p>	<p>Стаття 33. Державний нагляд (контроль) за дотриманням вимог законодавства у сфері електронних довірчих послуг</p> <p>5. За результатами проведення перевірок кваліфікованих надавачів електронних довірчих послуг (їхніх відокремлених пунктів реєстрації), засвідчувального центру, центрального засвідчувального органу контролюючий орган вживає таких заходів реагування:</p> <p>3) надсилає центральному засвідчувальному органу подання про виключення кваліфікованого надавача електронних довірчих послуг з Довірчого списку в разі:</p> <p>надання кваліфікованих електронних довірчих послуг за відсутності у кваліфікованого надавача електронних довірчих послуг поточного рахунка із спеціальним режимом використання у банку (рахунок в органі, що здійснює казначейське обслуговування бюджетних коштів) з необхідним обсягом коштів або чинного договору</p>

	страхування цивільно-правової відповідальності з необхідним розміром страхової суми, що встановлені частиною третьою статті 16 цього Закону, для забезпечення відшкодування збитків, які можуть бути завдані користувачам електронних довірчих послуг або третім особам внаслідок неналежного виконання кваліфікованим надавачем електронних довірчих послуг своїх зобов'язань;
24. Керівник та інші посадові особи акредитованого центру, які безпосередньо беруть участь в обслуговуванні посилених сертифікатів ключів (далі - посадові особи), повинні мати відповідний досвід роботи не менше ніж три роки.	<p>Стаття 30. Набуття статусу кваліфікованого надавача електронних довірчих послуг</p> <p>2. Юридичні особи, фізичні особи - підприємці для внесення відомостей про них до Довірчого списку подають до центрального засвідчувального органу або засвідчувального центру:</p> <p>6) засвідчені в установленому законодавством порядку копії документів, які підтверджують освітньо-кваліфікаційний рівень та трирічний стаж роботи за фахом найманих працівників, обов'язки яких будуть безпосередньо пов'язані з наданням кваліфікованих електронних довірчих послуг;</p>
<p>25. <i>Обов'язковими в акредитованому центрі є посади адміністратора реєстрації, адміністратора сертифікації, адміністратора безпеки та системного адміністратора.</i></p> <p><i>Адміністратор реєстрації відповідає за встановлення фізичних та юридичних осіб, фізичних осіб - підприємців під час формування, блокування, поновлення та скасування сертифіката.</i></p> <p><i>Адміністратор сертифікації відповідає за формування сертифікатів, списків відкликаних сертифікатів, збереження та використання особистого ключа</i></p>	

<p><i>акредитованого центру.</i></p> <p><i>Адміністратор безпеки відповідає за належне функціонування комплексної системи захисту інформації та входить до складу служби захисту інформації акредитованого центру. Забороняється суміщення посади адміністратора безпеки з іншими посадами.</i></p> <p><i>Системний адміністратор відповідає за функціонування програмно-технічного комплексу.</i></p>	
<p>26. Керівник та посадові особи акредитованого центру несуть відповідальність за розголошення конфіденційної інформації, зокрема відомостей про персональні дані, згідно із законом.</p>	<p>Стаття 13. Права та обов'язки кваліфікованих надавачів електронних довірчих послуг</p> <p>2. Кваліфіковані надавачі електронних довірчих послуг зобов'язані забезпечити:</p> <p>захист персональних даних користувачів електронних довірчих послуг відповідно до вимог законодавства;</p> <p>інформування контролюючого органу про порушення конфіденційності та/або цілісності інформації, що впливають на надання електронних довірчих послуг або стосуються персональних даних користувачів електронних довірчих послуг, не пізніше 24 годин з моменту, коли їм стало відомо про таке порушення;</p> <p>інформування користувачів електронних довірчих послуг про порушення конфіденційності та/або цілісності інформації, що впливають на надання їм електронних довірчих послуг або стосуються їхніх персональних даних, не пізніше двох годин з моменту, коли їм стало відомо про такі порушення.</p>
<p>27. Акредитований центр під час надання послуги</p>	<p>Стаття 23. Кваліфіковані сертифікати відкритих</p>

<p>сертифікації фізичним та юридичним особам зобов'язаний:</p> <p>генерувати відкритий та особистий ключі підписувача;</p> <p>формувати сертифікат згідно із законом.</p> <p>Під час формування сертифіката акредитований центр:</p> <p>присвоює унікальний реєстраційний номер сертифікату;</p> <p>перевіряє унікальність відкритого ключа підписувача в реєстрі чинних, блокованих та скасованих сертифікатів;</p> <p>включає дані про обмеження використання електронного цифрового підпису;</p> <p>включає електронну адресу електронного інформаційного ресурсу, де публікується список відкликаних сертифікатів акредитованого центру;</p> <p>на вимогу підписувача включає додаткові дані.</p> <p><i>Сертифікат підписувача, сформований акредитованим центром, чинний не більше ніж два роки.</i></p> <p><i>Сертифікат акредитованого центру чинний не більше ніж п'ять років.</i></p>	<p>ключів</p> <p>1. Під час надання кваліфікованих електронних довірчих послуг використовуються кваліфіковані сертифікати електронного підпису, кваліфіковані сертифікати електронної печатки та кваліфіковані сертифікати автентифікації веб-сайту.</p> <p>2. Кваліфіковані сертифікати відкритих ключів обов'язково повинні містити:</p> <p>1) позначку, що сертифікат відкритого ключа виданий як кваліфікований сертифікат відкритого ключа;</p> <p>2) позначку, що сертифікат відкритого ключа виданий в Україні;</p> <p>3) ідентифікаційні дані, які однозначно визначають кваліфікованого надавача електронних довірчих послуг, засвідчувальний центр або центральний засвідчувальний орган, які видали кваліфікований сертифікат відкритого ключа (далі - суб'єкти, які видали сертифікат), у тому числі обов'язково:</p> <p>для юридичної особи: найменування та код згідно з Єдиним державним реєстром підприємств та організацій України, за якими здійснено її державну реєстрацію;</p> <p>для фізичної особи - підприємця: прізвище, ім'я, по батькові (за наявності) та унікальний номер запису в Єдиному державному демографічному реєстрі або реєстраційний номер облікової картки платника податків, або серія та номер паспорта (для фізичних осіб, які через</p>
--	--

свої релігійні переконання відмовляються від прийняття реєстраційного номера облікової картки платника податків та повідомили про це відповідний орган доходів і зборів та мають відмітку в паспорті про право здійснювати платежі за серією та номером паспорта), за якими здійснено її державну реєстрацію;

4) ідентифікаційні дані, які однозначно визначають користувача електронних довірчих послуг, у тому числі обов'язково:

прізвище, ім'я, по батькові (за наявності) підписувача та унікальний номер запису в Єдиному державному демографічному реєстрі або реєстраційний номер облікової картки платника податків, або серія та номер паспорта (для фізичних осіб, які через свої релігійні переконання відмовляються від прийняття реєстраційного номера облікової картки платника податків та повідомили про це відповідний орган доходів і зборів та мають відмітку в паспорті про право здійснювати платежі за серією та номером паспорта) або;

найменування або прізвище, ім'я, по батькові (за наявності) створювача електронної печатки та код згідно з Єдиним державним реєстром підприємств та організацій України, за якими здійснено його державну реєстрацію, або унікальний номер запису в Єдиному державному демографічному реєстрі, або реєстраційний номер облікової картки платника податків, або серія та номер паспорта (для фізичних осіб, які через свої релігійні переконання відмовляються від прийняття реєстраційного номера облікової картки платника податків та повідомили про це відповідний орган доходів і зборів та мають відмітку в

паспорті про право здійснювати платежі за серією та номером паспорта);

5) місцезнаходження юридичної особи, якій видано кваліфікований сертифікат відкритого ключа;

6) значення відкритого ключа, який відповідає особистому ключу;

7) відомості про початок та закінчення строку дії кваліфікованого сертифіката відкритого ключа;

8) серійний номер кваліфікованого сертифіката відкритого ключа, унікальний для суб'єкта, який видав сертифікат;

9) кваліфікований електронний підпис або кваліфіковану електронну печатку, створені суб'єктом, який видав сертифікат;

10) відомості щодо розміщення у вільному доступі кваліфікованих сертифікатів відкритих ключів суб'єкта, який видав сертифікат;

11) відомості щодо розміщення інформації, необхідної для отримання кваліфікованої електронної довірчої послуги формування, перевірки та підтвердження чинності кваліфікованих сертифікатів відкритих ключів;

12) відомості про те, що особистий ключ зберігається в засобі кваліфікованого електронного підпису чи печатки (для кваліфікованого сертифіката електронного підпису чи печатки);

13) відомості про обмеження використання кваліфікованого електронного підпису чи печатки (для кваліфікованого сертифіката електронного підпису чи печатки);

14) ім'я (імена) домену, що належить фізичній або юридичній особі, якій видано сертифікат відкритого ключа (для кваліфікованого сертифіката автентифікації веб-сайту).

3. Кваліфіковані сертифікати відкритих ключів можуть містити інші ідентифікаційні дані фізичних або юридичних осіб, необов'язкові додаткові спеціальні атрибути, визначені у стандартах для кваліфікованих сертифікатів відкритих ключів. Ці атрибути не повинні впливати на інтероперабельність і визнання кваліфікованих електронних підписів.

4. Обов'язкові вимоги до кваліфікованих сертифікатів відкритих ключів, а також порядок перевірки їх дотримання встановлюються Кабінетом Міністрів України.

5. Правочин, вчинений в електронній формі, може бути визнаний судом недійсним у разі, коли під час його вчинення використовувався кваліфікований електронний підпис чи печатка, кваліфікований сертифікат якого/якої не містить відомостей, передбачених частиною другою цієї статті, або містить недостовірні відомості.

<p>28. Особистий ключ акредитованого центру використовується виключно для формування сертифікатів підписувачів, даних про статус сертифіката та надання послуги фіксування часу.</p> <p>Після закінчення терміну чинності особистий ключ та всі його резервні копії знищуються методом, що не допускає можливості їх відновлення.</p>	
<p>29. Резервні копії сертифікатів та списку відкликаних сертифікатів, сформованих в акредитованому центрі, зберігаються в приміщенні, територіально відокремленому від приміщення акредитованого центру, із забезпеченням захисту від несанкціонованого доступу.</p>	
<p>30. Акредитований центр зобов'язаний забезпечити можливість цілодобового вільного доступу користувачів з використанням телекомунікаційних мереж загального користування до:</p> <p>сертифікатів підписувачів за їх згодою;</p> <p>даних про статус сертифікатів ключів;</p> <p>сертифіката акредитованого центру;</p> <p>нормативних документів з питань надання послуг електронного цифрового підпису, зокрема до правил посиленої сертифікації та регламенту роботи акредитованого центру, а також порядку здійснення перевірки чинності сертифіката.</p> <p>Надання користувачам достовірних даних про статус сертифікатів здійснюється за їх запитом у реальному часі та/або з використанням списку відкликаних сертифікатів</p>	<p>Стаття 13. Права та обов'язки кваліфікованих надавачів електронних довірчих послуг</p> <p>2. Кваліфіковані надавачі електронних довірчих послуг зобов'язані забезпечити:</p> <p>можливість цілодобового доступу до реєстру чинних, блокованих та скасованих сертифікатів відкритих ключів та до інформації про статус сертифікатів відкритих ключів через телекомунікаційні мережі загального користування;</p> <p>цілодобовий прийом та перевірку заяв підписувачів та створювачів електронних печаток про скасування, блокування та поновлення їхніх сертифікатів відкритих ключів;</p>

<p>відповідно до регламенту роботи акредитованого центру.</p> <p>31. Акредитований центр зобов'язаний забезпечити:</p> <p>цілодобовий прийом звернень про скасування та блокування сертифікатів;</p> <p>прийом звернень про поновлення сертифікатів;</p> <p>перевірку законності звернень про блокування, поновлення та скасування сертифікатів.</p> <p>Час між отриманням звернення підписувача або його уповноваженого представника про скасування, блокування сертифіката та внесенням змін до списку відкликаних сертифікатів, доступних користувачам, не повинен перевищувати двох годин.</p> <p>Час формування, скасування, блокування та поновлення сертифікатів встановлюється за київським часом і синхронізується з Всесвітнім координованим часом (UTC) з точністю до однієї секунди.</p> <p>Формування, скасування, блокування та поновлення сертифікатів здійснюється за участю або під контролем не менше ніж двох посадових осіб акредитованого центру відповідно до їх посадових обов'язків.</p>	<p>Стаття 13. Права та обов'язки кваліфікованих надавачів електронних довірчих послуг</p> <p>2. Кваліфіковані надавачі електронних довірчих послуг зобов'язані забезпечити:</p> <p>захист персональних даних користувачів електронних довірчих послуг відповідно до вимог законодавства;</p> <p>функціонування програмно-технічного комплексу, що ними використовується, та захист інформації, що в ньому обробляється, відповідно до вимог законодавства;</p> <p>створення та функціонування свого веб-сайту;</p> <p>впровадження, підтримання в актуальному стані та публікацію на своєму веб-сайті реєстру чинних, блокованих та скасованих сертифікатів відкритих ключів;</p> <p>можливість цілодобового доступу до реєстру чинних, блокованих та скасованих сертифікатів відкритих ключів та до інформації про статус сертифікатів відкритих ключів через телекомунікаційні мережі загального користування;</p> <p>цілодобовий прийом та перевірку заяв підписувачів та створювачів електронних печаток про скасування, блокування та поновлення їхніх сертифікатів відкритих ключів;</p> <p>скасування, блокування та поновлення сертифікатів відкритих ключів відповідно до вимог цього Закону;</p>
--	---

встановлення під час формування сертифіката відкритого ключа належності відкритого ключа та відповідного йому особистого ключа підписувачу чи створювачу електронної печатки;

внесення ідентифікаційних даних підписувача чи створювача електронної печатки до відповідного сертифіката відкритого ключа;

інформування контролюючого органу про порушення конфіденційності та/або цілісності інформації, що впливають на надання електронних довірчих послуг або стосуються персональних даних користувачів електронних довірчих послуг, не пізніше 24 годин з моменту, коли їм стало відомо про таке порушення;

інформування користувачів електронних довірчих послуг про порушення конфіденційності та/або цілісності інформації, що впливають на надання їм електронних довірчих послуг або стосуються їхніх персональних даних, не пізніше двох годин з моменту, коли їм стало відомо про такі порушення;

унеможливлення використання особистого ключа у разі його компрометації;

постійне зберігання всіх виданих кваліфікованих сертифікатів відкритих ключів;

внесення коштів на поточний рахунок із спеціальним режимом використання у банку (рахунок в органі, що здійснює казначейське обслуговування бюджетних коштів) або страхування цивільно-правової відповідальності для

забезпечення відшкодування шкоди, яка може бути заподіяна користувачам таких послуг чи третім особам внаслідок неналежного виконання кваліфікованим надавачем електронних довірчих послуг своїх зобов'язань, у розмірі, визначеному частиною третьою статті 16 цього Закону;

наймання працівників, які володіють необхідними для надання кваліфікованих електронних довірчих послуг знаннями, досвідом і кваліфікацією, у тому числі у сферах інформаційних технологій та захисту інформації;

використання під час надання електронних довірчих послуг виключно кваліфікованих сертифікатів, засвідчених у центральному засвідчувальному органі чи засвідчувальному центрі;

зберігання документів, поданих користувачами для отримання електронних довірчих послуг;

інформування контролюючого органу та центрального засвідчувального органу або засвідчувального центру про будь-які зміни у процедурі надання електронних довірчих послуг протягом 48 годин з моменту настання таких змін;

передачу центральному засвідчувальному органу або засвідчувальному центру документованої інформації в разі припинення діяльності з надання електронних довірчих послуг.

*32. У договорі між акредитованим центром та підписувачем щодо надання послуг електронного цифрового підпису **додатково** зазначається про згоду або незгоду підписувача надавати вільний доступ до його сертифіката*

Стаття 29. Особливості надання кваліфікованих електронних довірчих послуг центральним засвідчувальним органом

2. Договір про надання центральним засвідчувальним

<p><i>користувачам та порядок взаємодії між підписувачем і акредитованим центром.</i></p>	<p>органом кваліфікованої електронної довірчої послуги формування, перевірки та підтвердження чинності кваліфікованого сертифіката електронного підпису чи печатки повинен містити умови щодо:</p> <p>підстав для внесення змін або розірвання договору про надання центральним засвідчувальним органом кваліфікованої електронної довірчої послуги формування, перевірки та підтвердження чинності кваліфікованого сертифіката електронного підпису чи печатки.</p>
<p>33. Акредитований центр може надавати інші послуги, які не суперечать вимогам законодавства та цього Порядку.</p>	
<p>34. Захист інформації, яка обробляється в акредитованому центрі, забезпечується в результаті здійснення комплексу технічних, криптографічних, організаційних та інших заходів і впровадження комплексної системи захисту інформації.</p>	
<p>35. Комплексна система захисту інформації повинна мати атестат відповідності вимогам захисту інформації.</p>	
<p>36. В акредитованому центрі створюється служба захисту інформації, яка забезпечує вирішення питань, пов'язаних із проектуванням, розробленням і модернізацією, введенням в експлуатацію, обслуговуванням і підтримкою працездатності комплексної системи захисту інформації, а також контролем за станом захищеності інформації.</p>	