

ПОРІВНЯЛЬНА ТАБЛИЦЯ

<p style="text-align: center;">Постанова Кабінету Міністрів України від 28 жовтня 2004 року № 1452 «Про затвердження Порядку застосування електронного цифрового підпису органами державної влади, органами місцевого самоврядування, підприємствами, установами та організаціями державної форми власності»</p>	<p style="text-align: center;">Постанова Кабінету Міністрів України від 19 вересня 2018 року № 749 «Про затвердження Порядку використання електронних довірчих послуг в органах державної влади, органах місцевого самоврядування, підприємствах, установах та організаціях державної форми власності»</p>
<p>1. Цей Порядок визначає вимоги до застосування електронного цифрового підпису органами державної влади, органами місцевого самоврядування, підприємствами, установами та організаціями державної форми власності (далі – установи).</p>	<p>1. Цей Порядок визначає вимоги щодо використання, у тому числі отримання, кваліфікованих електронних довірчих послуг в органах державної влади, органах місцевого самоврядування, підприємствах, установах та організаціях державної форми власності (далі – державні установи) із використанням працівниками державних установ засобів кваліфікованого електронного підпису.</p>
<p style="text-align: center;">_____</p>	<p>2. У цьому Порядку терміни вживаються у такому значенні:</p> <p style="padding-left: 40px;">захищений носій особистих ключів – засіб кваліфікованого електронного підпису чи печатки, що призначений для зберігання особистого ключа та має вбудовані апаратно-програмні засоби, що забезпечують захист записаних на ньому даних від несанкціонованого доступу, безпосереднього ознайомлення із значенням параметрів особистих ключів та їх копіювання;</p> <p style="padding-left: 40px;">інформаційний обмін – відправлення, отримання та передача електронних документів, що здійснюється користувачем кваліфікованих електронних довірчих послуг в електронній формі за допомогою засобів інформаційних, телекомунікаційних, інформаційно-телекомунікаційних систем або шляхом відправлення електронних носіїв, на яких записано цей документ;</p> <p style="padding-left: 40px;">кваліфіковані електронні довірчі послуги – електронні</p>

	<p>довірчі послуги, що надаються кваліфікованим надавачем електронних довірчих послуг відповідно до Закону України «Про електронні довірчі послуги».</p> <p>Інші терміни вживаються у значенні, наведеному у Законі України «Про електронні довірчі послуги».</p>
<p>2. Установа застосовує електронний цифровий підпис лише за умови використання надійних засобів електронного цифрового підпису, що повинне бути підтверджено сертифікатом відповідності або позитивним експертним висновком за результатами державної експертизи у сфері криптографічного захисту інформації, отриманим на ці засоби від Адміністрації Держспецзв'язку, та наявності посиленних сертифікатів відкритих ключів у своїх працівників – підписувачів.</p> <p>Для вчинення правочинів, надання адміністративних та інших послуг в електронній формі, здійснення інформаційного обміну з іншими юридичними особами установи використовують виключно захищені носії з урахуванням вимог, передбачених абзацом першим цього пункту.</p>	<p>4. Державні установи для засвідчення чинності відкритого ключа використовують лише кваліфікований сертифікат відкритого ключа, а для здійснення повноважень, спрямованих на набуття, зміну чи припинення прав та/або обов'язків фізичної або юридичної особи відповідно до закону, здійснення інформаційного обміну з іншими юридичними особами, – виключно захищені носії особистих ключів.</p> <p>У кваліфікованому сертифікаті відкритого ключа підписувача додатково до ідентифікаційних даних фізичної особи зазначаються ідентифікаційні дані державної установи (найменування та код згідно з ЄДРПОУ, за якими здійснено державну реєстрацію установи).</p>
3. Пункт 3 виключено	_____
4. Пункт 4 виключено	_____
<p>5. Установа отримує на договірних засадах послуги електронного цифрового підпису від акредитованих центрів сертифікації ключів. Один і той самий відкритий ключ підписувача повинен бути засвідчений лише в одному акредитованому центрі сертифікації ключів.</p>	<p>3. Державна установа отримує на договірних засадах такі кваліфіковані електронні довірчі послуги:</p> <p>створення, проведення перевірки та підтвердження кваліфікованого електронного підпису чи печатки;</p> <p>формування, проведення перевірки та підтвердження чинності кваліфікованого сертифіката електронного підпису чи печатки;</p> <p>формування, проведення перевірки та підтвердження чинності кваліфікованого сертифіката автентифікації веб-</p>

	<p>сайту; формування, проведення перевірки та підтвердження кваліфікованої електронної позначки часу; здійснення реєстрованої електронної доставки; зберігання кваліфікованих електронних підписів, печаток, позначок часу та сертифікатів, пов'язаних з цими послугами. Закупівля кваліфікованих електронних довірчих послуг здійснюється відповідно до Закону України «Про публічні закупівлі».</p>
6. Пункт 6 виключено	_____
7. Пункт 7 виключено	_____
8. Відповідальність за організацію застосування електронного цифрового підпису в установі несе її керівник, якщо інше не встановлено законодавством.	13. Відповідальність за організацію використання, у тому числі отримання, кваліфікованих електронних довірчих послуг у державній установі несе її керівник, якщо інше не встановлено законом.
<p>9. Застосування електронного цифрового підпису в установі забезпечує підрозділ інформаційних технологій, а у разі відсутності такого – підрозділ, що виконує відповідні функції (далі – відповідальний підрозділ), або працівник, спеціально визначений рішенням цієї установи (її керівника). Зазначений підрозділ (працівник) забезпечує:</p> <p>підготовку та подання акредитованому центру сертифікації ключів інформації, необхідної для отримання послуг, пов'язаних з електронним цифровим підписом; надання допомоги підписувачам під час генерації їх особистих та відкритих ключів; подання до акредитованого центру сертифікації ключів звернень про скасування, блокування або поновлення посилених сертифікатів відкритих ключів підписувачів; доступ підписувачів через телекомунікаційні мережі до</p>	<p>6. Організацію використання кваліфікованих електронних довірчих послуг у державній установі забезпечує відповідальний підрозділ, що виконує відповідні функції, або працівник, визначений рішенням такої установи (її керівника). Відповідальний підрозділ (працівник) забезпечує:</p> <p>підготовку та подання кваліфікованому надавачу інформації, необхідної для отримання кваліфікованих електронних довірчих послуг; надання допомоги підписувачам під час генерації їх особистих та відкритих ключів; ознайомлення підписувачів з правилами застосування кваліфікованих електронних довірчих послуг та здійснення контролю за їх дотриманням; взаємодію з кваліфікованим надавачем з питань</p>

<p>акредитованих центрів сертифікації ключів у разі неможливості здійснення ними такого доступу із своїх робочих місць;</p> <p>ведення обліку надійних засобів електронного цифрового підпису та носіїв, на яких зберігаються особисті ключі підписувачів;</p> <p>ведення обліку програмно-апаратних та апаратних носіїв особистих ключів підписувачів;</p> <p>зберігання документів та їх електронних копій, на підставі яких отримано послуги, пов'язані з електронним цифровим підписом;</p> <p>контроль за використанням підписувачами надійних засобів електронного цифрового підпису та зберіганням ними особистих ключів.</p>	<p>використання кваліфікованих електронних довірчих послуг;</p> <p>подання кваліфікованому надавачу заяв про скасування, блокування або поновлення кваліфікованих сертифікатів відкритих ключів;</p> <p>ведення обліку захищених носіїв особистих ключів та засобів кваліфікованого електронного підпису чи печатки;</p> <p>зберігання оригіналів документів та/або їх копій (крім копій особистих документів підписувачів, що містять їх персональні дані), на підставі яких отримано кваліфіковані електронні довірчі послуги;</p> <p>здійснення контролю за використанням підписувачами засобів кваліфікованого електронного підпису чи печатки та зберіганням ними особистих ключів.</p>
<p>Для подання акредитованому центру сертифікації ключів інформації, необхідної для отримання послуг електронного цифрового підпису, установа може використовувати систему електронної взаємодії органів виконавчої влади у разі:</p> <p>використання такої системи акредитованим центром сертифікації ключів;</p> <p>дотримання вимог щодо захисту інформації в такій системі установою та акредитованим центром сертифікації ключів.</p>	<p>8. Для подання кваліфікованому надавачу інформації, необхідної для отримання кваліфікованих електронних довірчих послуг, державна установа може використовувати систему електронної взаємодії органів виконавчої влади у разі:</p> <p>використання такої системи кваліфікованим надавачем;</p> <p>дотримання вимог щодо захисту інформації в такій системі державною установою та кваліфікованим надавачем.</p>
<p>10. Порядок надання працівникам установи права застосування електронного цифрового підпису, ведення обліку, зберігання та знищення їх особистих ключів, а також надання акредитованому центру сертифікації ключів інформації, необхідної для формування, скасування, блокування або поновлення посилених сертифікатів</p>	<p>5. Вимоги щодо ведення обліку, зберігання та знищення особистих ключів працівників державної установи, а також надання кваліфікованому надавачу електронних довірчих послуг (далі – кваліфікований надавач) інформації, необхідної для формування, скасування, блокування або поновлення кваліфікованих сертифікатів відкритих ключів</p>

<p>відкритих ключів підписувачів установи, визначається наказом її керівника, якщо інше не встановлено законодавством.</p>	<p>підписувачів державної установи, визначаються рішенням державної установи (її керівника), якщо інше не встановлено законом.</p>
<p>11. Генерація особистого та відкритого ключів здійснюється підписувачем в акредитованому центрі сертифікації ключів, що обслуговує установу, або безпосередньо в установі з використанням надійних засобів електронного цифрового підпису. У разі потреби під час генерації особистого та відкритого ключів підписувачеві надається допомога персоналом відповідального підрозділу (працівником) або персоналом акредитованого центру сертифікації ключів із дотриманням вимог щодо недопущення ознайомлення з особистим ключем підписувача осіб, що надають таку допомогу.</p>	<p>7. Ідентифікація підписувача – представника державної установи, проведення перевірки цивільної правоздатності та дієздатності державної установи здійснюються відповідно до вимог статті 22 Закону України «Про електронні довірчі послуги».</p> <p>Подання кваліфікованому надавачу інформації, необхідної для отримання кваліфікованих електронних довірчих послуг, здійснюється відповідальним підрозділом (працівником) або підписувачем особисто.</p> <p>Генерація пари ключів (особистого та відкритого) здійснюється підписувачем із використанням засобів кваліфікованого електронного підпису за його особистої присутності у кваліфікованого надавача, що обслуговує державну установу, або безпосередньо в державній установі.</p>
<p>12. У посиленому сертифікаті відкритого ключа підписувача додатково зазначаються ідентифікаційні дані установи (повне найменування та код згідно з ЄДРПОУ, за якими здійснено її державну реєстрацію).</p>	<p>Абзац другий пункту 4 Порядку.</p> <p>У кваліфікованому сертифікаті відкритого ключа підписувача додатково до ідентифікаційних даних фізичної особи зазначаються ідентифікаційні дані державної установи (найменування та код згідно з ЄДРПОУ, за якими здійснено державну реєстрацію установи).</p>
<p>13. У разі коли згідно із законодавством необхідно засвідчити печаткою справжність підпису на документах та відповідність копій документів оригіналам, а також для забезпечення цілісності електронних даних та ідентифікації установи як підписувача під час надання адміністративних та інших послуг в електронній формі, здійснення інформаційного обміну з іншими юридичними особами установа застосовує спеціально призначений для таких цілей</p>	<p>11. Для визначення достовірності походження та проведення перевірки цілісності електронних даних, а також ідентифікації державної установи як підписувача, у тому числі для засвідчення відповідності електронних копій електронного та паперового (фотокопія) документів оригіналу у випадках, передбачених законодавством, установа застосовує кваліфіковану електронну печатку. При цьому кваліфікована електронна печатка створюється за</p>

<p>електронний цифровий підпис (далі – електронна печатка).</p> <p>У посиленому сертифікаті відкритого ключа, що використовується установою для електронної печатки, додатково зазначаються спеціальне призначення електронного цифрового підпису та сфера його застосування.</p>	<p>допомогою захищених носіїв особистих ключів.</p> <p>Перелік електронних документів, які потребують засвідчення електронною печаткою, визначається інструкцією з діловодства державної установи.</p> <p>Рішенням державної установи (її керівника) визначаються необхідність використання кваліфікованої електронної печатки та уповноважені посадові особи, відповідальні за її застосування.</p>
<p>14. Перелік працівників установи, яким надається право накладення електронної печатки на електронних документах, визначається рішенням установи (її керівника).</p> <p>Отримання в акредитованому центрі сертифікації ключів посиленого сертифіката відкритого ключа для забезпечення застосування електронної печатки, а також генерація відповідних ключів здійснюється в тому ж порядку, що й для електронного цифрового підпису.</p>	<p>Абзац другий пункту 12 Порядку.</p> <p>У разі звільнення підписувача з державної установи або переведення до іншої державної установи підписувач або державна установа звертаються до кваліфікованого надавача для скасування його кваліфікованого сертифіката відкритого ключа із заявою, а особистий ключ знищується методом, що не допускає можливості його відновлення.</p>
<p>15. Підписувач використовує у процесі виконання своїх посадових обов’язків лише особистий ключ, отриманий відповідно до пунктів 10 та 11 цього Порядку.</p> <p>Після припинення виконання підписувачем посадових обов’язків, для яких генерувалися особистий та відкритий ключі, підписувач або установа звертається до акредитованого центру сертифікації ключів для скасування посиленого сертифіката його відкритого ключа, а особистий ключ знищується методом, що не допускає можливості його відновлення.</p>	<p>Абзац перший пункту 12 Порядку.</p> <p>Скасування та блокування кваліфікованих сертифікатів відкритих ключів державних установ здійснюються у випадках, за умов та у порядку, що визначені у статті 25 Закону України «Про електронні довірчі послуги».</p>
<p>16. Підставами для блокування та/або скасування посиленого сертифіката відкритого ключа підписувача є:</p> <ul style="list-style-type: none"> звільнення; відсторонення від виконання повноважень; смерть; набрання законної сили рішенням суду про оголошення його померлим, визнання його безвісно відсутнім, 	

<p>недієздатним, обмеження його цивільної дієздатності; подання заяви про блокування та/або скасування сертифіката у зв'язку з підтвердженням факту компрометації особистого ключа; зміна даних, внесених до посиленого сертифіката відкритого ключа.</p>	
<p>17. Підписувач для виконання своїх посадових обов'язків не може використовувати одночасно кілька чинних посилених сертифікатів одного відкритого ключа.</p>	
<p>18. Підписувач і працівник установи, якому надано право накладення електронної печатки на електронних документах, несуть відповідальність за зберігання особистих ключів, паролів та кодів доступу до них.</p>	<p>6. Організацію використання кваліфікованих електронних довірчих послуг у державній установі забезпечує відповідальний підрозділ, що виконує відповідні функції, або працівник, визначений рішенням такої установи (її керівника). Відповідальний підрозділ (працівник) забезпечує:</p>
<p>19. Передача особистих ключів іншим особам забороняється.</p>	<p>підготовку та подання кваліфікованому надавачу інформації, необхідної для отримання кваліфікованих електронних довірчих послуг; надання допомоги підписувачам під час генерації їх особистих та відкритих ключів; ознайомлення підписувачів з правилами застосування кваліфікованих електронних довірчих послуг та здійснення контролю за їх дотриманням; взаємодію з кваліфікованим надавачем з питань використання кваліфікованих електронних довірчих послуг; подання кваліфікованому надавачу заяв про скасування, блокування або поновлення кваліфікованих сертифікатів відкритих ключів; ведення обліку захищених носіїв особистих ключів та засобів кваліфікованого електронного підпису чи печатки; зберігання оригіналів документів та/або їх копій (крім копій особистих документів підписувачів, що містять їх персональні дані), на підставі яких отримано кваліфіковані електронні довірчі послуги;</p>

<p>20. Ідентифікація підписувача та підтвердження цілісності даних в електронній формі здійснюються шляхом перевірки електронного цифрового підпису, накладеного на такі дані. Електронний цифровий підпис вважається таким, що пройшов перевірку, якщо:</p> <p>перевірку електронного цифрового підпису проведено з використанням надійного засобу електронного цифрового підпису;</p> <p>у результаті перевірки встановлено, що на момент накладення електронного цифрового підпису був чинним посилений сертифікат відкритого ключа підписувача, посилений сертифікат відкритого ключа акредитованого центру сертифікації ключів, посилений сертифікат відкритого ключа відповідного засвідчувального центру та посилений сертифікат відкритого ключа центрального засвідчувального органу;</p> <p>під час перевірки підтверджено цілісність даних, на які накладено електронний цифровий підпис.</p>	<p>здійснення контролю за використанням підписувачами засобів кваліфікованого електронного підпису чи печатки та</p> <p>9. Ідентифікація підписувача та підтвердження цілісності даних в електронній формі, з якими пов'язаний кваліфікований електронний підпис чи печатка, здійснюються шляхом перевірки кваліфікованого електронного підпису чи печатки.</p> <p>Кваліфікований електронний підпис чи печатка вважаються такими, що пройшли перевірку та отримали підтвердження, якщо:</p> <p>перевірку кваліфікованого електронного підпису чи печатки проведено засобом кваліфікованого електронного підпису чи печатки;</p> <p>перевіркою встановлено, що відповідно до вимог Закону України «Про електронні довірчі послуги» на момент створення кваліфікованого електронного підпису чи печатки був чинним кваліфікований сертифікат електронного підпису чи печатки підписувача чи створювача електронної печатки;</p> <p>за допомогою кваліфікованого сертифіката електронного підпису чи печатки здійснено ідентифікацію підписувача чи створювача електронної печатки;</p> <p>під час проведення перевірки за допомогою кваліфікованого сертифіката електронного підпису чи печатки отримано підтвердження того, що особистий ключ, який належить підписувачу чи створювачу електронної печатки, зберігається в засобі кваліфікованого електронного підпису чи печатки, у тому числі на захищеному носіїві особистого ключа у випадках, передбачених пунктом 4 цього Порядку;</p> <p>під час проведення перевірки підтверджено цілісність</p>

	даних в електронній формі, з якими пов'язаний кваліфікований електронний підпис чи печатка.
_____	10. Використання електронної позначки часу під час накладання кваліфікованого електронного підпису чи печатки є обов'язковим.
21. Контроль за виконанням в установах вимог цього Порядку здійснює Адміністрація Держспецзв'язку.	14. Державний нагляд (контроль) за дотриманням у державних установах вимог цього Порядку здійснює Держспецзв'язку.
_____	15. Інші обов'язкові вимоги щодо використання, у тому числі отримання, кваліфікованих електронних довірчих послуг у державних установах, а також порядок проведення перевірки їх дотримання визначаються відповідно до положень Закону України «Про електронні довірчі послуги».