затверджено

МІНІСТЕРСТВО ЮСТИЦІЇ УКРАЇНИ

вул. Городецького, 13, м. Київ, 01001
Тел.: +380 44 278-37-23, факс: + 380 44 271-17-83
E-mail: themis@minjust.gov.ua
http://www.minjust.gov.ua
Код ЄДРПОУ 00015622

Державна регуляторна служба України

_____ № _____

На № _____

Щодо погодження проекту постанови Кабінету Міністрів України

Міністерством юстиції України відповідно до статей 13, 18, 19, 20, 21, 23, 26, 27, 28, 33 Закону України «Про електронні довірчі послуги» розроблено проект постанови Кабінету Міністрів України «Про затвердження Вимог у сфері електронних довірчих послуг та Порядку перевірки дотримання вимог законодавства у сфері електронних довірчих послуг» (далі – проект Постанови).

Проект Постанови розміщено на офіційному веб-сайті Міністерства юстиції України в підрубриці «Повідомлення про оприлюднення регуляторних актів, що розроблені Міністерством юстиції» підрубрики «Регуляторна діяльність» рубрики «Напрями діяльності».

Враховуючи викладене, просимо погодити проект Постанови.

Додатки:
1. Проект Постанови на 59 арк. в 1 прим.
2. Пояснювальна записка на 14 арк. в 1 прим.
3. Аналіз регуляторного впливу на 15 арк. в 1 прим.
4. Повідомлення про оприлюднення на 1 арк. в 1 прим.

Директор Департаменту приватного права **Олена ФЕРЕНС**

148678

Сергій Ісаєнко 486 87 24

ПРОЕКТ

КАБІНЕТ МІНІСТРІВ УКРАЇНИ

ПОСТАНОВА

від _____ 2018 р. № _____

Київ

Про затвердження Вимог у сфері електронних довірчих послуг та Порядку перевірки дотримання вимог законодавства у сфері електронних довірчих послуг

Відповідно до статей 13, 18, 19, 20, 21, 23, 26, 27, 28, 33 Закону України «Про електронні довірчі послуги» Кабінет Міністрів України **постановляє:**

1. Затвердити такі, що додаються:

Вимоги у сфері електронних довірчих послуг;

Порядок перевірки дотримання вимог законодавства у сфері електронних довірчих послуг.

2. Визнати такими, що втратили чинність, постанови Кабінету Міністрів України згідно з переліком, що додається.

3. Ця постанова набирає чинності з дня наступного за днем її опублікування, але не раніше дня набрання чинності Законом України «Про електронні довірчі послуги», крім пунктів 60 – 64 Переліку стандартів, що застосовуються кваліфікованими надавачами електронних довірчих послуг під час надання кваліфікованих електронних довірчих послуг, який додається до Вимог у сфері електронних довірчих послуг, що набирають чинності з 01 січня 2019 року.

Прем'єр-міністр України **В. ГРОЙСМАН**

ЗАТВЕРДЖЕНО
постановою Кабінету Міністрів України
від 2018 р. №

ВИМОГИ
у сфері електронних довірчих послуг

Розділ І. Загальні положення

1. Сфера дії

1. Вимоги до надання кваліфікованих електронних довірчих послуг визначають організаційно-методологічні технічні та технологічні умови, яких повинен дотримуватись кваліфікований надавач електронних довірчих послуг (далі – надавач), його відокремлені пункти реєстрації під час надання кваліфікованих електронних довірчих послуг їх користувачам.

2. Центральний засвідчувальний орган надає кваліфіковані електронні довірчі послуги відповідно до цих Вимог з урахуванням особливостей, передбачених Законом України «Про електронні довірчі послуги».

3. Дія цих Вимог не поширюється на надавачів електронних довірчих послуг, що не мають наміру надавати кваліфіковані електронні довірчі послуги, а також на надавачів, внесених до Довірчого списку за поданням засвідчувального центру, та програмно-технічні комплекси, що використовуються ними під час надання кваліфікованих електронних довірчих послуг у банківській системі України та при здійсненні переказу коштів.

2. Визначення термінів

4. Терміни, що вживаються в цих Вимогах, мають таке значення:

власник веб-сайту – користувач кваліфікованої електронної довірчої послуги формування, перевірки та підтвердження чинності кваліфікованого сертифіката автентифікації веб-сайту;

геш-значення – фіксовані за обсягом електронні дані, утворені шляхом перетворення електронних даних із застосуванням криптографічного алгоритму;

гешування – перетворення будь-якого обсягу електронних даних в електронні дані фіксованого обсягу шляхом застосування криптографічного алгоритму;

заявник – фізична особа або представник юридичної особи, що звернулась до надавача для отримання кваліфікованих електронних довірчих послуг;

інформаційно-телекомунікаційна система – сукупність інформаційних та телекомунікаційних систем надавача або центрального засвідчувального органу, які у процесі обробки інформації діють як єдине ціле та об'єднують програмно-технічний комплекс, що використовується під час надання кваліфікованих електронних довірчих послуг (далі – програмно-технічний комплекс), фізичне середовище, інформацію, що обробляється в цих системах, а також найманих працівників надавача або центрального засвідчувального органу, які безпосередньо задіяні у наданні кваліфікованих електронних довірчих послуг або обслуговують програмно-технічний комплекс (далі – наймані працівники);

кваліфікована електронна довірча послуга – електронна довірча послуга, надання якої забезпечує надавач, його відокремлені пункти реєстрації або центральний засвідчувальний орган за допомогою засобу кваліфікованого електронного підпису чи печатки та базується на кваліфікованому сертифікаті відкритого ключа;

користувач – особа, яка на підставі договору або іншого документа отримує у надавача кваліфіковану електронну довірчу послугу;

об'єктний ідентифікатор – унікальний буквено-числовий чи числовий ідентифікатор, зареєстрований у відповідному стандарті Міжнародної організації із стандартизації для певного класу об'єктів або об'єктів;

он-лайн операція – будь-яка дія, технологічна схема якої передбачає наявність безперервного телекомунікаційного зв'язку в режимі реального часу під час її виконання;

політика сертифіката (certificate policy) – перелік усіх правил, що застосовуються надавачем у процесі надання кваліфікованих електронних довірчих послуг з обслуговування кваліфікованих сертифікатів відкритих ключів, включаючи положення цих Вимог;

положення сертифікаційних практик (certification practice statement) – перелік усіх практичних дій та процедур, які застосовуються для реалізації політики сертифіката надавача;

публікація кваліфікованого сертифіката відкритого ключа – надання кваліфікованого сертифіката відкритого ключа користувачу та у разі його згоди іншим особам шляхом розміщення на офіційному веб-сайті надавача;

регламент роботи – нормативний документ надавача або центрального засвідчувального органу, що визначає організаційно-методологічні, технічні та технологічні умови діяльності надавача або центрального засвідчувального органу під час надання кваліфікованих електронних довірчих послуг, включаючи політику сертифіката та положення сертифікаційних практик;

розповсюдження інформації про статус кваліфікованого сертифіката відкритого ключа – надання вільного доступу до інформації про статус кваліфікованого сертифіката відкритого ключа;

список відкликаних сертифікатів – сформований та опублікований надавачем перелік кваліфікованих сертифікатів відкритих ключів, статус яких змінено на блокований, поновлений або скасований;

статус кваліфікованого сертифіката відкритого ключа – стан кваліфікованого сертифіката відкритого ключа (чинний, блокований, скасований) на певний момент часу;

управління статусом сертифіката – зміна статусу кваліфікованого сертифіката відкритого ключа надавачем.

5. Інші терміни вживаються у значеннях, наведених у законах України «Про електронні довірчі послуги», «Про електронні документи та електронний документообіг», «Про телекомунікації», «Про захист інформації в інформаційно-телекомунікаційних системах», «Про основні засади забезпечення кібербезпеки України».

Розділ ІІ. Вимоги до надавачів

1. Вимоги до найманих працівників надавача

1. До посад найманих працівників надавача, обов'язки яких безпосередньо пов'язані з наданням кваліфікованих електронних довірчих послуг, належать:

1) адміністратор реєстрації;

2) адміністратор сертифікації;

3) адміністратор безпеки;

4) системний адміністратор;

5) адміністратор аудиту.

Забороняється суміщення посади адміністратора безпеки та адміністратора аудиту з іншими посадами найманих працівників надавача, обов'язки яких безпосередньо пов'язані з наданням кваліфікованих електронних довірчих послуг.

2. Наймані працівники надавача повинні мати необхідні для надання кваліфікованих електронних довірчих послуг знання, досвід і кваліфікацію.

На посаду адміністратора сертифікації, адміністратора безпеки, системного адміністратора та адміністратора аудиту може бути призначена особа, яка має вищу освіту за спеціальністю у сферах інформаційних технологій, захисту інформації або кібербезпеки, а також стаж роботи за фахом в зазначених сферах не менше 3 років.

3. Організаційно-правовий статус керівника та найманих працівників надавача, їх функції та завдання, права та обов'язки, відповідальність в межах організації, а також професійні знання, досвід та кваліфікацію визначають посадові інструкції.

Посадові інструкції повинні містити вимоги інформаційної безпеки та методи її забезпечення.

4. Керівник та наймані працівники надавача повинні бути ознайомлені з положеннями їх посадових інструкції та діяти відповідно до своїх посадових функцій та завдань.

5. Адміністратор реєстрації відповідає за перевірку документів, наданих заявниками, їх заяв про формування, блокування, поновлення та скасування кваліфікованих сертифікатів відкритих ключів.

6. Основними обов'язками адміністратора реєстрації є:

1) ідентифікація та автентифікація заявників;

2) перевірка заяв про формування, блокування, поновлення та скасування кваліфікованих сертифікатів відкритих ключів;

3) встановлення належності відкритого ключа та відповідного йому особистого ключа заявнику;

4) ведення обліку користувачів.

7. Адміністратор сертифікації відповідає за формування кваліфікованих сертифікатів відкритих ключів, ведення електронного реєстру чинних, блокованих та скасованих сертифікатів відкритих ключів, збереження та використання особистих ключів надавача, а також створення їх резервних копій.

8. Основними обов'язками адміністратора сертифікації є:

1) участь у генерації пар ключів надавача та створенні резервних копій особистих ключів надавача;

2) зберігання особистих ключів надавача та їх резервних копій;

3) забезпечення використання особистих ключів надавача під час формування та обслуговування кваліфікованих сертифікатів відкритих ключів надавача та користувачів;

4) перевірка заяв про формування кваліфікованих сертифікатів відкритих ключів надавача вимогам регламенту роботи центрального засвідчувального органу;

5) участь у знищенні особистих ключів надавача;

6) забезпечення ведення, архівування та відновлення баз даних кваліфікованих сертифікатів відкритих ключів користувачів;

7) забезпечення публікації кваліфікованих сертифікатів відкритих ключів користувачів та списків відкликаних сертифікатів на офіційному веб-сайті надавача;

8) створення резервних копій кваліфікованих сертифікатів відкритих ключів користувачів;

9) зберігання кваліфікованих сертифікатів відкритих ключів користувачів, їх резервних копій, списків відкликаних сертифікатів та інших важливих ресурсів інформаційно-телекомунікаційної системи надавача.

9. Адміністратор безпеки відповідає за належне функціонування комплексної системи захисту інформації або системи управління інформаційною безпекою.

10. Основними обов'язками адміністратора безпеки є:

1) участь у генерації пар ключів надавача та створенні резервних копій особистих ключів надавача;

2) контроль за формуванням, обслуговуванням та створенням резервних копій кваліфікованих сертифікатів відкритих ключів надавача, користувачів та списків відкликаних сертифікатів;

3) контроль за зберіганням особистих ключів надавача та їх резервних копій, особистих ключів адміністраторів;

4) участь у знищенні особистих ключів надавача, контроль за правильним і своєчасним знищенням адміністраторами їх особистих ключів;

5) організація розмежування доступу до ресурсів інформаційно-телекомунікаційної системи надавача;

6) забезпечення спостереження за функціонуванням комплексної системи захисту інформації або системи управління інформаційною безпекою (реєстрація подій в інформаційно-телекомунікаційній системі надавача, моніторинг подій тощо);

7) забезпечення організації та проведення заходів з модернізації, тестування, оперативного відновлення функціонування комплексної системи

захисту інформації або системи управління інформаційною безпекою після збоїв, відмов, аварій інформаційно-телекомунікаційної системи надавача;

8) забезпечення режиму доступу до приміщень надавача, в яких розміщена інформаційно-телекомунікаційна система надавача;

9) ведення журналів обліку адміністратора безпеки, передбачених документацією на комплексну систему захисту інформації або звітності, що передбачена системою управління інформаційною безпекою.

11. Системний адміністратор відповідає за функціонування засобів та обладнання програмно-технічного комплексу (далі – технічні засоби) інформаційно-телекомунікаційної системи надавача.

12. Основними обов'язками системного адміністратора є:

1) організація експлуатації та технічного обслуговування інформаційно-телекомунікаційної системи надавача і адміністрування її технічних засобів;

2) забезпечення функціонування офіційного веб-сайту надавача;

3) участь у впровадженні та забезпеченні функціонування комплексної системи захисту інформації або системи управління інформаційною безпекою;

4) ведення журналів аудиту подій, що реєструють технічні засоби інформаційно-телекомунікаційної системи надавача;

5) встановлення, налаштування та забезпечення підтримки працездатності загальносистемного та спеціального програмного забезпечення інформаційно-телекомунікаційної системи надавача;

6) встановлення та налагодження штатної підсистеми резервного копіювання бази даних інформаційно-телекомунікаційної системи надавача;

7) забезпечення актуалізації баз даних, створюваних та оброблюваних в інформаційно-телекомунікаційній системі надавача, внаслідок збоїв.

13. Адміністратор аудиту відповідає за здійснення перевірок дотримання найманими працівниками надавача вимог внутрішньої організаційно-розпорядчої документації надавача та документації на комплексну систему захисту інформації або систему управління інформаційною безпекою. Надавач встановлює періодичність (у днях, тижнях або місяцях) проведення таких внутрішніх перевірок, але не рідше ніж один раз на 6 місяців.

14. Обов'язки адміністратора аудиту:

1) здійснення перевірок журналів аудиту подій, що реєструють технічні засоби інформаційно-телекомунікаційної системи надавача;

2) здійснення перевірок відповідності внутрішньої організаційно-розпорядчої документації надавача та документації на комплексну систему захисту інформації або систему управління інформаційною безпекою;

3) контроль за дотриманням найманими працівниками надавача внутрішньої організаційно-розпорядчої документації надавача та документації

на комплексну систему захисту інформації або систему управління інформаційною безпекою;

4) контроль за веденням баз даних надавача;

5) контроль за веденням архіву надавача.

15. Наймані працівники надавача повинні бути повідомлені про зміни в організації процесів надавача, що стосуються їх посадових обов'язків.

16. Керівник надавача зобов'язаний створити умови для безперервної особистої освіти та забезпечити постійне підвищення кваліфікації найманих працівників надавача у сферах інформаційних технологій, захисту інформації або кібербезпеки та захисту персональних даних.

17. Керівником надавача має бути встановлена чітка система дисциплінарних стягнень за недотримання найманими працівниками надавача своїх посадових обов'язків, вимог нормативно-правових актів у сфері електронних довірчих послуг та вимог внутрішньої організаційно-розпорядчої документації надавача та документації на комплексну систему захисту інформації або систему управління інформаційною безпекою.

2. Вимоги до використання особистих ключів надавача

18. Генерація пари ключів надавача здійснюється адміністратором сертифікації під контролем адміністратора безпеки.

Генерація пари ключів надавача здійснюється виключно за допомогою засобу кваліфікованого електронного підпису чи печатки, що є апаратно-програмним або апаратним пристроєм.

19. Всі події, пов'язані із генерацією, використанням та знищенням пари ключів надавача, повинні протоколюватися.

20. Особисті ключі надавача повинні розміщуватися у засобі кваліфікованого електронного підпису чи печатки, що є апаратно-програмним або апаратним пристроєм, за допомогою якого здійснювалася генерація пари ключів.

Технологія зберігання особистих ключів надавача повинна забезпечити неможливість доступу до них ззовні у відношенні до засобу кваліфікованого електронного підпису чи печатки, що є апаратно-програмним або апаратним пристроєм.

21. У разі здійснення резервного копіювання особисті ключі надавача повинні бути перенесені на зовнішній носій (пристрій) у захищеному вигляді, що забезпечує їх цілісність та конфіденційність.

Резервне копіювання та відновлення особистих ключів надавача здійснюється адміністратором сертифікації під контролем адміністратора безпеки.

22. Умови забезпечення захисту резервних копій особистих ключів надавача під час їх зберігання повинні бути не нижче, ніж умови забезпечення захисту особистих ключів, що знаходяться у використанні.

23. Особисті ключі надавача можуть використовуватися виключно для формування кваліфікованих сертифікатів відкритих ключів (накладання кваліфікованого електронного підпису чи печатки на кваліфікований сертифікат відкритого ключа) та інформації про статус кваліфікованого сертифіката відкритого ключа.

24. Особисті ключі надавача можуть використовуватися виключно у засобі кваліфікованого електронного підпису чи печатки, що є апаратно-програмним або апаратним пристроєм, розташованим в окремому, спеціально призначеному для цього, приміщенні.

25. Після закінчення терміну дії кваліфікованого сертифіката відкритого ключа надавача особистий ключ надавача та всі його резервні копії знищуються способом, що не дозволяє їх відновлення.

3. Вимоги щодо страхування від збитків, які можуть бути завдані надавачем внаслідок неналежного виконання зобов'язань

26. Діяльність надавачів 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 збитків, які можуть бути завдані користувачам чи третім особам внаслідок неналежного виконання надавачем своїх зобов'язань.

27. Розмір внеску на поточному рахунку із спеціальним режимом використання у банку (рахунку в органі, що здійснює казначейське обслуговування бюджетних коштів) або страхової суми визначено частиною третьою статті 16 Закону України «Про електронні довірчі послуги».

28. Надавач зобов'язаний підтримувати розмір внеску на поточному рахунку із спеціальним режимом використання у банку (рахунку в органі, що здійснює казначейське обслуговування бюджетних коштів) або страхової суми в актуальному стані відповідно до розміру мінімальної заробітної плати, встановленого законом про Державний бюджет України на відповідний рік.

29. У разі відшкодування збитків, завданих користувачам чи третім особам внаслідок неналежного виконання своїх зобов'язань, надавач вживає вичерпних заходів для найшвидшого відновлення розміру внеску на поточному

рахунку із спеціальним режимом використання у банку (рахунку в органі, що здійснює казначейське обслуговування бюджетних коштів) або страхової суми.

4. Вимоги до регламенту роботи надавача

30. Надавач надає кваліфіковані електронні довірчі послуги відповідно до вимог законодавства у сфері електронних довірчих послуг та регламенту роботи надавача.

31. Регламент роботи надавача розробляється та затверджується до початку роботи надавача.

32. У регламенті роботи надавача повинно бути визначено:

1) загальні відомості про надавача (найменування або прізвище, ім'я, по батькові надавача; код за Єдиним державним реєстром підприємств та організацій України; місцезнаходження, номери телефонів, електронна адреса веб-сайту);

2) перелік кваліфікованих електронних довірчих послуг, надання яких забезпечує надавач;

3) посадовий склад надавача та функції найманих працівників надавача;

4) політика сертифіката та положення сертифікаційних практик;

5) опис процедур та процесів, які виконуються під час надання кваліфікованих електронних довірчих послуг, що не передбачають формування та обслуговування кваліфікованих сертифікатів відкритих ключів.

33. Політика сертифіката може описувати кожну кваліфіковану електронну довірчу послугу, що передбачає формування та обслуговування надавачем кваліфікованих сертифікатів відкритих ключів, окремо або у сукупності.

Положення сертифікаційних практик описують практичні та процедурні засади реалізації всіх політик сертифіката у сукупності.

34. У політиці сертифіката визначається:

1) сфера використання кваліфікованих сертифікатів відкритих ключів:

а) перелік сфер, у яких дозволяється використання кваліфікованих сертифікатів відкритих ключів, сформованих надавачем;

б) обмеження щодо використання кваліфікованих сертифікатів відкритих ключів, сформованих надавачем;

2) порядок розповсюдження інформації надавачем:

а) перелік інформації, що розміщується надавачем на своєму офіційному веб-сайті;

б) час і порядок публікації кваліфікованих сертифікатів відкритих ключів та списків відкликаних сертифікатів;

3) порядок ідентифікації та автентифікації заявників:

а) механізми підтвердження володіння заявником особистим ключем, відповідний якому відкритий ключ надається для формування кваліфікованого сертифіката відкритого ключа;

б) умови встановлення заявника (інформація, що надається заявником під час ідентифікації особи, види документів, на підставі яких встановлюється заявник, вимоги щодо особистої присутності);

в) механізми автентифікації користувачів, які мають чинний кваліфікований сертифікат відкритого ключа, сформований надавачем;

г) механізми автентифікації користувачів з питань блокування, скасування або поновлення кваліфікованого сертифіката відкритого ключа;

4) управління та операційний контроль:

а) фізичне середовище (опис приміщень надавача, в яких розміщена інформаційно-телекомунікаційна система надавача, механізми контролю доступу до них);

б) процедурний контроль (система дисциплінарних стягнень за недотримання найманими працівниками надавача своїх посадових обов'язків, вимог нормативно-правових актів у сфері електронних довірчих послуг та вимог внутрішньої організаційно-розпорядчої документації надавача та документації на комплексну систему захисту інформації або систему управління інформаційною безпекою в межах організації з урахуванням режиму роботи надавача);

в) ведення журналів аудиту подій (типи подій, що фіксуються у журналі аудиту подій, частота перегляду, строки зберігання журналів аудиту подій, захист та резервне копіювання журналів аудиту подій, перелік найманих працівників надавача, що можуть здійснювати перегляд журналів аудиту подій);

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

5) управління парами ключів:

а) генерація пар ключів (процес, порядок та умови генерації пар ключів надавача та користувачів);

б) процедури отримання користувачем особистого ключа в результаті надання кваліфікованої електронної довірчої послуги її надавачем;

в) механізм надання відкритого ключа користувача надавачу для формування кваліфікованого сертифіката відкритого ключа;

6) забезпечення захисту особистого ключа надавача:

а) порядок захисту та доступу до особистого ключа надавача;

б) резервне копіювання особистого ключа надавача, порядок та умови збереження, доступу та використання резервної копії.

35. У положеннях сертифікаційних практик має бути зазначено умови, процедури та механізми, пов'язані з формуванням, блокуванням, скасуванням та використанням кваліфікованого сертифіката відкритого ключа:

1) процес подання запиту на формування кваліфікованого сертифіката відкритого ключа (перелік суб'єктів, уповноважених здійснювати запит на формування кваліфікованого сертифіката відкритого ключа, порядок подачі та оброблення такого запиту, строки оброблення запиту на формування кваліфікованого сертифіката відкритого ключа);

2) надання сформованого кваліфікованого сертифіката відкритого ключа користувачу;

3) публікація сформованого кваліфікованого сертифіката відкритого ключа користувача на офіційному веб-сайті надавача;

4) умови використання кваліфікованого сертифіката відкритого ключа користувача та його особистого ключа (попередження про можливі наслідки неправильного використання кваліфікованого сертифіката відкритого ключа та особистого ключа);

5) процедура подачі запиту на формування кваліфікованого сертифіката відкритого ключа для користувачів, які мають чинний кваліфікований сертифікат відкритого ключа, сформований цим надавачем;

6) обставини скасування (блокування, поновлення) кваліфікованого сертифіката відкритого ключа; перелік суб'єктів, уповноважених здійснювати запит на скасування (блокування та поновлення) кваліфікованого сертифіката відкритого ключа; процедура подання запиту на скасування (блокування, поновлення) кваліфікованого сертифіката відкритого ключа; час оброблення запиту на скасування (блокування, поновлення) кваліфікованого сертифіката відкритого ключа; частота формування списку відкликаних сертифікатів та строки його дії; можливість та умови надання інформації про статус кваліфікованого сертифіката відкритого ключа у режимі реального часу);

7) закінчення строку чинності кваліфікованого сертифіката відкритого ключа користувача.

36. Проект регламенту роботи надавача підлягає обов'язковому погодженню з контролюючим органом.

Після погодження з контролюючим органом регламент роботи надавача затверджується його керівником у двох примірниках.

Один примірник погодженого з контролюючим органом та затвердженого керівником надавача регламенту роботи надавача передається до контролюючого органу.

37. Погодження та затвердження змін до регламенту роботи надавача здійснюється відповідно до вимог, передбачених для погодження та затвердження регламенту роботи надавача.

Для погодження змін до регламенту роботи надавача до контролюючого органу надається текст відповідних змін та порівняльна таблиця.

38. Надавач самостійно визначає обсяг положень регламенту його роботи та інших документів, що підлягають розміщенню на офіційному веб-сайті надавача для ознайомлення.

5. Вимоги до початку роботи надавача

39. Для набуття статусу надавача юридична особа або фізична особа – підприємець, що має намір надавати кваліфіковані електронні довірчі послуги, подає до центрального засвідчувального органу заяву про внесення відомостей про неї до Довірчого списку та інші документи, визначені частиною другою статті 30 Закону України «Про електронні довірчі послуги».

Форма заяви про внесення відомостей про юридичну особу або фізичну особу – підприємця до Довірчого списку встановлюється у регламенті роботи центрального засвідчувального органу.

40. Заява про внесення відомостей про юридичну особу або фізичну особу – підприємця до Довірчого списку та документи, що до неї додаються, можуть бути подані представником юридичної особи або фізичною особою – підприємцем, що має намір надавати кваліфіковані електронні довірчі послуги, в електронній формі через Єдиний державний портал адміністративних послуг, у тому числі через інтегровану з ним інформаційну систему центрального засвідчувального органу.

Забезпечення цілісності та конфіденційності інформації, у тому числі персональних даних, під час подання заяви повинно здійснюватись з дотриманням вимог законодавства у сфері захисту інформації із застосуванням кваліфікованого електронного підпису представника юридичної особи або фізичної особи – підприємця та з використання засобів шифрування, що мають позитивний експертний висновок за результатами державної експертизи у сфері криптографічного захисту інформації.

У разі подання документів для внесення відомостей про юридичну особу або фізичну особу – підприємця до Довірчого списку в електронній формі копії документів, які існують виключно в паперовій формі, додаються до заяви про внесення до Довірчого списку у форматі PDF.

Відповідність оригіналам копій документів засвідчується шляхом накладення кваліфікованого електронного підпису керівника юридичної особи або фізичної особи – підприємця, що має намір надавати кваліфіковані електронні довірчі послуги.

Представник юридичної особи або фізична особа – підприємець, що має намір надавати кваліфіковані електронні довірчі послуги, відповідає за достовірність інформації наданої в документах для внесення відомостей про юридичну особу або фізичну особу – підприємця до Довірчого списку.

У разі подання заяви про внесення відомостей про юридичну особу або фізичну особу – підприємця до Довірчого списку та документів, що до неї додаються, в електронній формі документи на паперових носіях не подаються.

Уповноважена особа центрального засвідчувального органу перевіряє надходження електронних документів не рідше двох разів на день (у першій та другій половині робочого дня).

Документи для внесення відомостей про юридичну особу або фізичну особу – підприємця до Довірчого списку, подані в електронній формі, реєструються в інформаційній системі центрального засвідчувального органу після їх надходження, про що автоматично через персональний кабінет на Єдиному державному порталі адміністративних послуг інформується представник юридичної особи або фізична особа – підприємець, що має намір надавати кваліфіковані електронні довірчі послуги.

41. Після вжиття вичерпних заходів для забезпечення ідентифікації та перевірки обсягу цивільної правоздатності та дієздатності представника юридичної особи або фізичної особи – підприємця, що має намір надавати кваліфіковані електронні довірчі послуги, центральний засвідчувальний орган здійснює розгляд заяви про внесення відомостей про юридичну особу або фізичну особу – підприємця до Довірчого списку та документів, що до неї додаються, і за результатами їх розгляду приймає рішення в порядку та у строки, встановлені Законом України «Про електронні довірчі послуги».

42. На підставі прийнятого центральним засвідчувальним органом рішення про внесення до Довірчого списку юридична особа або фізична особа – підприємець, що має намір надавати кваліфіковані електронні довірчі послуги, засвідчує чинність одного або декількох своїх відкритих ключів (окремо для кожної кваліфікованої електронної довірчої послуги) у центральному засвідчувальному органі відповідно до вимог регламенту роботи центрального засвідчувального органу.

Засвідчення чинності відкритого ключа юридичної особи або фізичної особи – підприємця є умовою внесення до Довірчого списку інформації про кваліфіковані електронні довірчі послуги, які має намір надавати юридична особа або фізична особа – підприємець.

Для засвідчення чинності відкритого ключа юридична особа або фізична особа – підприємець подає до центрального засвідчувального органу:

1) заяву про формування кваліфікованого сертифіката відкритого ключа та відповідний їй електронний запит, що формується після генерації пари ключів;

2) підписаний примірник договору про надання центральним засвідчувальним органом кваліфікованої електронної довірчої послуги формування, перевірки та підтвердження чинності кваліфікованого сертифіката електронного підпису чи печатки.

43. Юридична особа або фізична особа – підприємець, що має намір надавати кваліфіковані електронні довірчі послуги, набуває статус надавача з дня внесення відомостей про неї до Довірчого списку.

44. Рішення центрального засвідчувального органу про внесення відомостей про юридичну особу або фізичну особу – підприємця до Довірчого списку оприлюднюється на офіційному веб-сайті центрального засвідчувального органу, а представник юридичної особи або фізична особа – підприємець, що має намір надавати кваліфіковані електронні довірчі послуги, повідомляється центральним засвідчувальним органом про прийняте рішення шляхом надсилання листа поштою або в електронній формі через персональний кабінет на Єдиному державному порталі адміністративних послуг.

45. Зміна відомостей про надавача, що містяться в Довірчому списку, є підставою для внесення змін до Довірчого списку, яке здійснюється в порядку та у строки, встановлені Законом України «Про електронні довірчі послуги».

У разі виникнення змін у відомостях, внесених до Довірчого списку, надавач зобов'язаний протягом п'яти робочих днів з дня настання таких змін подати до центрального засвідчувального органу заяву про внесення змін до Довірчого списку разом з документами, що підтверджують відповідні зміни.

6. Вимоги до припинення діяльності з надання кваліфікованих електронних довірчих послуг

46. Надавач припиняє діяльність з надання кваліфікованих електронних довірчих послуг з підстав та в порядку, що визначені статтею 31 Закону України «Про електронні довірчі послуги».

47. У разі припинення надання кваліфікованих електронних довірчих послуг надавач зобов'язаний передати центральному засвідчувальному органу документовану інформацію (документи, на підставі яких користувачам надавалися кваліфіковані електронні довірчі послуги та були сформовані, блоковані, поновлені, скасовані кваліфіковані сертифікати відкритих ключів, усі сформовані кваліфіковані сертифікати відкритих ключів, а також реєстри сформованих кваліфікованих сертифікатів відкритих ключів) у порядку, визначеному Кабінетом Міністрів України.

48. Передавання документованої інформації здійснюється надавачем не пізніше дня, визначеного ним як дата припинення діяльності з надання кваліфікованих електронних довірчих послуг, чи дня набрання законної сили відповідним рішенням суду.

49. Центральний засвідчувальний орган скасовує виданий ним кваліфікований сертифікат відкритого ключа надавача у день, визначений надавачем як дата припинення діяльності з надання кваліфікованих електронних довірчих послуг, чи у день набрання законної сили відповідним рішенням суду.

III. Вимоги до надання кваліфікованих електронних довірчих послуг

1. Загальні вимоги до надавача під час надання кваліфікованих електронних довірчих послуг

1. Кваліфіковані електронні довірчі послуги користувачам надають виключно надавачі.

2. Надавач може надавати окремо або в сукупності:

1) кваліфіковану електронну довірчу послугу створення, перевірки та підтвердження кваліфікованого електронного підпису чи печатки;

2) кваліфіковану електронну довірчу послугу формування, перевірки та підтвердження чинності кваліфікованого сертифіката електронного підпису чи печатки;

3) кваліфіковану електронну довірчу послугу формування, перевірки та підтвердження чинності кваліфікованого сертифіката автентифікації веб-сайту;

4) кваліфіковану електронну довірчу послугу формування, перевірки та підтвердження кваліфікованої електронної позначки часу;

5) кваліфіковану електронну довірчу послугу реєстрованої електронної доставки;

6) кваліфіковану електронну довірчу послугу зберігання кваліфікованих електронних підписів, печаток, електронних позначок часу та сертифікатів, пов'язаних з цими послугами.

3. Приміщення, у яких здійснюється обслуговування користувачів, повинні бути доступними для осіб з обмеженими фізичними можливостями відповідно до державних будівельних норм, правил і стандартів.

Інформація про умови доступності спеціальних приміщень для осіб з обмеженими фізичними можливостями розміщується у місці, доступному для візуального сприйняття користувачів.

4. Для надання кваліфікованої електронної довірчої послуги надавач здійснює ідентифікацію заявника шляхом перевірки ідентифікаційних даних особи з документів, що надаються заявником, та даних одержаних з інформаційних систем органів державної влади.

5. Ідентифікація заявника та перевірка обсягу його цивільної правоздатності та дієздатності здійснюється відповідно до вимог статті 22 Закону України «Про електронні довірчі послуги».

6. Ідентифікаційні дані особи, що надаються заявником для отримання кваліфікованої електронної довірчої послуги, повинні бути перевірені надавачем:

1) за особистої присутності заявника;

2) шляхом використання засобу електронної ідентифікації заявника, який було особисто отримано заявником та який має високий рівень довіри відповідно до схеми електронної ідентифікації, визначеної Кабінетом Міністрів України;

3) шляхом використання ідентифікаційних даних особи – заявника з чинного кваліфікованого сертифіката відкритого ключа, сформованого тим самим надавачем.

7. Заявник повинен надати інформацію, що дозволяє зв'язатися з ним та визначена регламентом роботи надавача.

8. Реєстрація користувачів може здійснюватися через відокремлені пункти реєстрації, які виконують свої функції згідно з регламентом роботи надавача.

9. Центральний засвідчувальний орган здійснює надання кваліфікованих електронних довірчих послуг надавачам відповідно до регламенту роботи центрального засвідчувального органу з дотриманням цих Вимог.

10. Надавач повинен забезпечити можливість ознайомлення заявників з інформацією про умови отримання кваліфікованої електронної довірчої послуги.

11. До інформації, вільний доступ до якої повинен забезпечити надавач, відносяться:

1) відомості про надавача;

2) інформація про внесення відомостей про надавача до Довірчого списку;

3) кваліфіковані сертифікати відкритих ключів надавача;

4) перелік кваліфікованих електронних довірчих послуг, які надає надавач;

5) інформація про засоби кваліфікованого електронного підпису чи печатки, що використовуються під час надання кваліфікованих електронних довірчих послуг;

6) форми документів, на підставі яких надаються кваліфіковані електронні довірчі послуги;

7) реєстр чинних, блокованих та скасованих сертифікатів відкритих ключів;

8) відомості про обмеження при використанні кваліфікованих сертифікатів відкритих ключів користувачами;

9) інформація щодо порядку перевірки чинності кваліфікованого сертифіката відкритого ключа, у тому числі умови перевірки статусу кваліфікованого сертифіката відкритого ключа;

10) законодавство в сфері електронних довірчих послуг.

12. Надавач забезпечує інформування користувачів щодо умов отримання кваліфікованих електронних довірчих послуг, у тому числі шляхом розміщення відповідної інформації на офіційному веб-сайті надавача.

Інформація на офіційному веб-сайті надавача повинна бути доступною для осіб з обмеженими фізичними можливостями.

13. Кваліфіковані електронні довірчі послуги надаються на підставі договору надавача із заявником про надання кваліфікованої електронної довірчої послуги.

Підставою надання кваліфікованих електронних довірчих послуг в органах державної влади, органах місцевого самоврядування, підприємствах, установах та організаціях державної форми власності може бути відповідне рішення керівника.

14. Надавач обліковує та зберігає протягом строків, визначених законодавством, договори про надання кваліфікованих електронних довірчих послуг, а також документи (засвідчені в установленому порядку копії документів), що використовуються під час ідентифікації та перевірки достатності обсягу цивільної правоздатності та дієздатності заявника.

15. Істотними умовами договору про надання кваліфікованих електронних довірчих послуг є:

1) права та обов'язки сторін;

2) умови використання засобів кваліфікованого електронного підпису чи печатки (у разі якщо кваліфікована електронна довірча послуга передбачає використання засобів кваліфікованого електронного підпису чи печатки);

3) умови використання заявником особистого ключа (у разі якщо кваліфікована електронна довірча послуга передбачає використання особистого ключа);

4) умови публікації кваліфікованого сертифіката відкритого ключа заявника (у разі якщо кваліфікована електронна довірча послуга передбачає формування кваліфікованого сертифіката відкритого ключа);

5) строк дії договору;

6) умови оплати;

7) порядок внесення змін до договору;

8) порядок розірвання договору.

16. Договір про надання кваліфікованої електронної довірчої послуги може бути змінено виключно за взаємною згодою сторін.

17. У разі зміни відомостей, що містяться у договорі про надання кваліфікованої електронної довірчої послуги, заявник у триденний строк з дня настання таких змін повідомляє про це надавача та надає документи, що підтверджують відповідні зміни.

18. Підставами для розірвання договору про надання кваліфікованої електронної довірчої послуги є:

1) згода сторін;

2) рішення суду про розірвання договору;

3) виключення надавача з Довірчого списку.

19. У разі якщо договір про надання кваліфікованої електронної довірчої послуги передбачав формування кваліфікованого сертифіката відкритого ключа, розірвання такого договору є підставою для скасування надавачем кваліфікованого сертифіката відкритого ключа, сформованого відповідно до такого договору.

20. Надавач має право самостійно обирати, які саме стандарти будуть ним застосовуватися при наданні кваліфікованих електронних довірчих послуг з Переліку, що додається до цих Вимог.

21. Контроль за наданням кваліфікованих електронних довірчих послуг надавачами здійснює контролюючий орган.

2. Вимоги до надання кваліфікованої електронної довірчої послуги створення, перевірки та підтвердження кваліфікованих електронних підписів чи печаток

22. Кваліфікована електронна довірча послуга створення, перевірки та підтвердження кваліфікованих електронних підписів чи печаток включає вчинення дій, передбачених частиною першою статті 18 Закону України «Про електронні довірчі послуги».

23. Під час надання кваліфікованої електронної довірчої послуги створення, перевірки та підтвердження кваліфікованих електронних підписів чи печаток надавачем забезпечується:

1) використання підписувачем або створювачем електронної печатки виключно засобу кваліфікованого електронного підпису чи печатки та кваліфікованого сертифіката електронного підпису чи печатки;

2) захист обміну інформацією між підписувачем або створювачем електронної печатки та надавачем засобами телекомунікаційних мереж загального користування;

3) створення умов для генерації пари ключів підписувача або створювача електронної печатки;

4) допомога під час генерації пари ключів підписувача або створювача електронної печатки у спосіб, що не допускає порушення конфіденційності та цілісності особистого ключа, а також ознайомлення із значенням параметрів особистого ключа та їх копіювання;

5) унікальності пари ключів підписувача або створювача електронної печатки;

6) зберігання особистого ключа підписувача або створювача електронної печатки;

7) захист від доступу сторонніх осіб до параметрів особистого ключа підписувача або створювача електронної печатки під час використання засобу кваліфікованого електронного підпису чи печатки.

24. У разі якщо пара ключів була згенерована заявником поза приміщенням надавача та/або за відсутності відповідного персоналу, ідентифікація такого заявника, перевірка достатності обсягу його цивільної правоздатності і дієздатності, формування та видача йому кваліфікованого сертифіката відкритого ключа здійснюється надавачем після перевірки володіння заявником особистим ключем, який відповідає відкритому ключу, наданому для формування кваліфікованого сертифіката відкритого ключа.

Перевірка володіння заявником особистим ключем виконується без розкриття його особистого ключа.

25. Генерацію та/або управління парою ключів від імені підписувача або створювача електронної печатки може здійснювати виключно надавач.

26. Надавач, який здійснює управління парою ключів підписувача або створювача електронної печатки, може здійснювати резервне копіювання особистого ключа підписувача або створювача електронної печатки з метою його зберігання за умови дотримання таких вимог:

1) рівень безпеки резервної копії особистого ключа повинен відповідати рівню безпеки оригінального особистого ключа;

2) кількість резервних копій не повинна перевищувати мінімального значення, необхідного для забезпечення безперервності послуги.

27. Кваліфікований електронний підпис чи печатка повинні відповідати таким вимогам:

1) встановлювати однозначний зв'язок з підписувачем або створювачем електронної печатки;

2) надавати можливість здійснити електронну ідентифікацію підписувача або створювача електронної печатки;

3) забезпечувати одноосібний контроль підписувача або створювача електронної печатки за відповідним особистим ключем;

4) виявляти будь-які зміни пов'язаних електронних даних, на які накладено кваліфікований електронний підпис чи печатку.

28. Процес перевірки кваліфікованого електронного підпису чи печатки повинен підтвердити справжність кваліфікованого електронного підпису чи печатки за таких умов:

1) дотримання вимог, визначених у частині другій статті 18 Закону України «Про електронні довірчі послуги»;

2) правильності внесення ідентифікаційних даних особи до відповідного кваліфікованого сертифіката електронного підпису чи печатки підписувача або створювача електронної печатки;

3) під час перевірки встановлено, що кваліфікований електронний підпис або печатку створено за допомогою засобу кваліфікованого електронного підпису чи печатки;

4) дотримання вимог, визначених у пункті 26 цього підрозділу, на момент накладення на пов'язані електронні дані.

29. Перевірка кваліфікованого електронного підпису чи печатки може здійснюватися будь-якою особою з метою отримання інформації про дійсність чи недійсність кваліфікованого електронного підпису чи печатки.

30. Надання кваліфікованої електронної довірчої послуги перевірки та підтвердження кваліфікованих електронних підписів чи печаток передбачає, що:

1) послуга надається виключно надавачем;

2) послуга відповідає всім вимогам до перевірки кваліфікованих електронних підписів чи печаток, визначеним у пункті 26 цього підрозділу;

3) дозволяє отримувати результати перевірки із застосуванням кваліфікованого електронного підпису чи печатки надавача автоматизованим способом, який є надійним, ефективним та захищеним.

3. Вимоги до надання кваліфікованої електронної довірчої послуги формування, перевірки та підтвердження чинності кваліфікованого сертифіката електронного підпису чи печатки

31. Кваліфікована електронна довірча послуга формування, перевірки та підтвердження чинності кваліфікованого сертифіката електронного підпису чи печатки включає вчинення дій, передбачених частиною першою статті 20 Закону України «Про електронні довірчі послуги».

32. Формування кваліфікованого сертифіката електронного підпису чи печатки заявника здійснюється надавачем на основі ідентифікаційних даних особи, одержаних від заявника під час його ідентифікації та перевірки достатності обсягу його цивільної правоздатності і дієздатності.

33. Надавач зобов'язаний забезпечити унікальність серійного номера кваліфікованого сертифіката електронного підпису чи печатки заявника серед інших кваліфікованих сертифікатів електронного підпису чи печатки, сформованих цим самим надавачем.

34. Надавач зобов'язаний резервувати всі сформовані ним кваліфіковані сертифікати електронного підпису чи печатки.

35. Під час повторного формування кваліфікованого сертифіката електронного підпису чи печатки користувача надавач повинен перевірити актуальність інформації, що надавалась для попереднього формування кваліфікованого сертифіката електронного підпису чи печатки цього заявника.

36. Кваліфікований сертифікат електронного підпису чи печатки користувача після його формування надавачем повинен бути доступний користувачу, для якого цей кваліфікований сертифікат електронного підпису чи печатки був сформований.

37. Доступ інших осіб до сформованого кваліфікованого сертифіката електронного підпису чи печатки користувача надається у разі його згоди на публікацію кваліфікованого сертифіката електронного підпису чи печатки.

38. У разі зміни відомостей, що містяться у кваліфікованому сертифікаті електронного підпису чи печатки, користувач у триденний строк з дня настання таких змін повідомляє про це надавача та надає документи, що підтверджують відповідні зміни.

На підставі наданих користувачем документів, що підтверджують зміни відомостей, що містяться у кваліфікованому сертифікаті електронного підпису чи печатки, надавач здійснює повторне формування кваліфікованого сертифіката електронного підпису чи печатки користувача та його публікацію у разі згоди користувача.

Повторне формування кваліфікованого сертифіката електронного підпису чи печатки користувача не продовжує строку дії його кваліфікованого сертифіката електронного підпису чи печатки.

39. Сформований кваліфікований сертифікат електронного підпису чи печатки користувача скасовується або блокується надавачем у разі настання підстав передбачених статтею 25 Закону України «Про електронні довірчі послуги».

40. Заява про скасування або блокування кваліфікованого сертифіката електронного підпису чи печатки подається користувачем надавачу в будь-який спосіб, що забезпечує підтвердження особи-користувача.

Під час опрацювання заяви про скасування або блокування кваліфікованого сертифіката електронного підпису чи печатки надавачем здійснюється ідентифікація та перевірка достатності обсягу цивільної правоздатності і дієздатності користувача з дотриманням вимог щодо підтвердження особи, встановлених у регламенті роботи надавача.

41. Кваліфікований сертифікат електронного підпису чи печатки користувача вважається скасованим або блокованим з моменту зміни надавачем статусу кваліфікованого сертифіката електронного підпису чи печатки користувача на скасований або блокований.

42. Користувач, статус кваліфікованого сертифіката електронного підпису чи печатки якого було змінено на скасований чи блокований, повинен невідкладно бути поінформований про відповідну зміну статусу.

43. Скасований кваліфікований сертифікат електронного підпису чи печатки поновленню не підлягає.

44. Відомості про кваліфіковані сертифікати електронного підпису чи печатки, сформовані надавачем, їх статус та списки відкликаних сертифікатів містяться у реєстрі чинних, блокованих та скасованих сертифікатів відкритих ключів.

45. Розповсюдження інформації про статус кваліфікованих сертифікатів електронного підпису чи печатки користувачів здійснюється за допомогою публікації повного та часткового списків відкликаних сертифікатів на офіційному веб-сайті надавача та забезпечення можливості перевірки статусу кваліфікованого сертифіката електронного підпису чи печатки користувача в режимі реального часу через телекомунікаційні мережі загального користування.

До списку відкликаних сертифікатів надавача висуваються такі вимоги:

1) у кожному списку відкликаних сертифікатів зазначається граничний термін його дії до видання наступного списку, якщо інше не передбачено регламентом роботи надавача;

Продовження додатка

Стандарти, що визначають вимоги до надання кваліфікованих електронних довірчих послуг, пов'язаних зі створенням, перевіркою та підтвердженням електронних підписів, печаток, а також зберіганням кваліфікованих електронних підписів, печаток, електронних позначок часу та відповідних сертифікатів відкритих ключів

6. ДСТУ ETSI TR 119 000:2017 «Електронні підписи та інфраструктури (ESI). Модель стандартизації підписів. Огляд», затверджений наказом державного підприємства «Український науково-дослідний і навчальний центр проблем стандартизації, сертифікації та якості» від 04 серпня 2017 року № 207 (ETSI TR 119 000:2016, IDT)
7. ДСТУ ETSI TR 119 001:2017 «Електронні підписи та інфраструктури (ESI). Модель стандартизації підписів. Визначення понять та скорочення», затверджений наказом державного підприємства «Український науково-дослідний і навчальний центр проблем стандартизації, сертифікації та якості» від 04 серпня 2017 року № 206 (ETSI TR 119 001:2016, IDT)
8. ДСТУ ETSI TR 119 100:2017 «Електронні підписи та інфраструктури (ESI). Настанова з використання стандартів для створення та валідації підпису», затверджений наказом державного підприємства «Український науково-дослідний і навчальний центр проблем стандартизації, сертифікації та якості» від 04 серпня 2017 року № 206 (ETSI TR 119 100:2016, IDT)
9. ДСТУ ETSI TS 119 101:2016 «Електронні підписи та інфраструктури. Вимоги та політики безпеки для додатків формування та перевірки підписів», затверджений наказом державного підприємства «Український науково-дослідний і навчальний центр проблем стандартизації, сертифікації та якості» від 23 вересня 2016 року № 279 (ETSI TS 119 101:2016, IDT)
10. ДСТУ ETSI EN 319 102-1:2016 «Електронні підписи й інфраструктури (ESI). Процедури створення та перевірення цифрового підпису ADES. Частина 1. Створення та перевіреннія», затверджений наказом державного підприємства «Український науково-дослідний і навчальний центр проблем стандартизації, сертифікації та якості» від 21 червня 2016 року № 183 (ETSI EN 319 102-1:2016, IDT)
11. ДСТУ ETSI EN 319 122-1:2016 «Електронні підписи й інфраструктури (ESI). Цифрові підписи CAdES. Частина 1. Структурні блоки та базові підписи CAdES», затверджений наказом державного підприємства «Український науково-дослідний і навчальний центр проблем стандартизації, сертифікації та якості» від 21 червня 2016 року № 183 (ETSI EN 319 122-1:2016, IDT)

Продовження додатка

12. ДСТУ ETSI EN 319 122-2:2016 «Електронні підписи й інфраструктури (ESI). Цифрові підписи CAdES. Частина 2. Розширені підписи CAdES», затверджений наказом державного підприємства «Український науково-дослідний і навчальний центр проблем стандартизації, сертифікації та якості» від 21 червня 2016 року № 183 (ETSI EN 319 122-2:2016, IDT)
13. ДСТУ ETSI EN 319 132-1:2016 «Електронні підписи й інфраструктури (ESI). Цифрові підписи XAdES. Частина 1. Структурні блоки та базові підписи XAdES», затверджений наказом державного підприємства «Український науково-дослідний і навчальний центр проблем стандартизації, сертифікації та якості» від 21 червня 2016 року № 183 (ETSI EN 319 132-1:2016, IDT)
14. ДСТУ ETSI EN 319 132-2:2016 «Електронні підписи й інфраструктури (ESI). Цифрові підписи XAdES. Частина 2. Розширені підписи XAdES», затверджений наказом державного підприємства «Український науково-дослідний і навчальний центр проблем стандартизації, сертифікації та якості» від 21 червня 2016 року № 183 (ETSI EN 319 132-2:2016, IDT)
15. ДСТУ ETSI EN 319 142-1:2016 «Електронні підписи та інфраструктури. Цифрові підписи PAdES. Частина 1. Структурні елементи та базові PAdES підписи», затверджений наказом державного підприємства «Український науково-дослідний і навчальний центр проблем стандартизації, сертифікації та якості» від 23 вересня 2016 року № 279 (ETSI EN 319 142-1:2016, IDT)
16. ДСТУ ETSI EN 319 142-2:2016 «Електронні підписи та інфраструктури. Цифрові підписи PAdES. Частина 2. Додаткові профілі підписів PAdES», затверджений наказом державного підприємства «Український науково-дослідний і навчальний центр проблем стандартизації, сертифікації та якості» від 23 вересня 2016 року № 279 (ETSI EN 319 142-2:2016, IDT)
17. ДСТУ ETSI EN 319 162-1:2016 «Електронні підписи й інфраструктури (ESI). Контейнери, пов'язані з підписом (ASiC). Частина 1. Структурні блоки та базові контейнери ASiC», затверджений наказом державного підприємства «Український науково-дослідний і навчальний центр проблем стандартизації, сертифікації та якості» від 21 червня 2016 року № 183 (ETSI EN 319 162-1:2016, IDT)
18. ДСТУ ETSI EN 319 162-2:2016 «Електронні підписи й інфраструктури (ESI). Контейнери, пов'язані з підписом (ASiC). Частина 2. Додаткові контейнери ASiC», затверджений наказом державного підприємства «Український науково-дослідний і навчальний центр проблем стандартизації, сертифікації та якості» від 21 червня 2016 року № 183 (ETSI EN 319 162-2:2016, IDT)

Продовження додатка

19. ДСТУ ETSI TS 102 778-1:2015 «Електронні підписи та інфраструктура (ESI). Профілі розширених електронних підписів PDF. Частина 1. Огляд серії PAdES – базові принципи PAdES», затверджений наказом державного підприємства «Український науково-дослідний і навчальний центр проблем стандартизації, сертифікації та якості» від 18 грудня 2015 року № 193 (ETSI TS 102 778-1:2009, IDT)
20. ДСТУ ETSI TS 102 778-2:2015 «Електронні підписи та інфраструктура (ESI). Профілі розширених електронних підписів PDF. Частина 2. Базовий PAdES – профілі, що базуються на ISO 32000-1», затверджений наказом державного підприємства «Український науково-дослідний і навчальний центр проблем стандартизації, сертифікації та якості» від 18 грудня 2015 року № 193 (ETSI TS 102 778-2:2009, IDT)
21. ДСТУ ETSI TS 102 778-3:2015 «Електронні підписи та інфраструктура (ESI). Профілі розширених електронних підписів PDF. Частина 3. Посилений PAdES – профілі PAdES-BES і PadES-EPES», затверджений наказом державного підприємства «Український науково-дослідний і навчальний центр проблем стандартизації, сертифікації та якості» від 18 грудня 2015 року № 193 (ETSI TS 102 778-3:2010, IDT)
22. ДСТУ ETSI TS 102 778-4:2015 «Електронні підписи та інфраструктура (ESI). Профілі розширених електронних підписів PDF. Частина 4. Довгостроковий PAdES – профіль PAdES LTV», затверджений наказом державного підприємства «Український науково-дослідний і навчальний центр проблем стандартизації, сертифікації та якості» від 18 грудня 2015 року № 193 (ETSI TS 102 778-4:2009, IDT)
23. ДСТУ ETSI TS 102 778-5:2015 «Електронні підписи та інфраструктура (ESI). Профілі розширених електронних підписів PDF. Частина 5. PAdES для XML контенту – профілі для підписів XAdES», затверджений наказом державного підприємства «Український науково-дослідний і навчальний центр проблем стандартизації, сертифікації та якості» від 18 грудня 2015 року № 193 (ETSI TS 102 778-5:2009, IDT)

Стандарти, що визначають вимоги до надання кваліфікованих електронних довірчих послуг, пов'язаних з формуванням, перевіркою та підтвердженням кваліфікованих сертифікатів електронного підпису, печатки, автентифікації веб-сайту

24. ДСТУ ETSI EN 319 411-1:2016 «Електронні підписи й інфраструктури (ESI). Вимоги політики та безпеки для провайдерів трастових послуг, які видають сертифікати. Частина 1. Загальні вимоги», затверджений наказом державного підприємства «Український науково-дослідний і навчальний центр проблем стандартизації, сертифікації та якості» від 21 червня 2016 року № 183 (ETSI EN 319 411-1:2016, IDT)

Продовження додатка

25. ДСТУ ETSI EN 319 411-2:2016 «Електронні підписи й інфраструктури (ESI). Вимоги політики та безпеки для провайдерів трастових послуг, які видають сертифікати. Частина 2. Вимоги до провайдерів трастових послуг, які видають кваліфіковані сертифікати ЄС», затверджений наказом державного підприємства «Український науково-дослідний і навчальний центр проблем стандартизації, сертифікації та якості» від 21 червня 2016 року № 183 (ETSI EN 319 411-2:2016, IDT)

Стандарти, що визначають вимоги до надання кваліфікованої електронної довірчої послуги формування, перевірки та підтвердження кваліфікованої електронної позначки часу

26. ДСТУ ETSI TS 101 861:2017 «Електронні підписи та інфраструктури (ESI). Профіль штемпелювання часу», затверджений наказом державного підприємства «Український науково-дослідний і навчальний центр проблем стандартизації, сертифікації та якості» від 09 серпня 2017 року № 214 (ETSI TS 101 861:2011, IDT)
27. ДСТУ ETSI EN 319 421:2016 «Електронні підписи й інфраструктури (ESI). Політика та вимоги безпеки щодо провайдерів трастових послуг, які видають часові штемпелі», затверджений наказом державного підприємства «Український науково-дослідний і навчальний центр проблем стандартизації, сертифікації та якості» від 21 червня 2016 року № 183 (ETSI EN 319 421:2016, IDT)
28. ДСТУ ETSI EN 319 422:2016 «Електронні підписи та інфраструктури. Протокол мітки часу та профілі токенів мітки часу», затверджений наказом державного підприємства «Український науково-дослідний і навчальний центр проблем стандартизації, сертифікації та якості» від 23 вересня 2016 року № 279 (ETSI EN 319 422:2016, IDT)

Стандарти, що визначають вимоги до засобів кваліфікованого електронного підпису чи печатки

29. ДСТУ EN 419211-1:2016 «Профілі захисту для пристроїв створення безпечного підпису. Частина 1. Огляд», затверджений наказом державного підприємства «Український науково-дослідний і навчальний центр проблем стандартизації, сертифікації та якості» від 23 вересня 2016 року № 279 (EN 419211-1:2014, IDT)
30. ДСТУ EN 419211-2:2016 «Профілі захисту для пристроїв створення безпечного підпису. Частина 2. Пристрій з генерацією ключів», затверджений наказом державного підприємства «Український науково-дослідний і навчальний центр проблем стандартизації, сертифікації та якості» від 23 вересня 2016 року № 279 (EN 419211-2:2013, IDT)

31. ДСТУ EN 419211-3:2016 «Профілі захисту для пристроїв створення безпечного підпису. Частина 3. Пристрій з імпортом ключів», затверджений наказом державного підприємства «Український науково-дослідний і навчальний центр проблем стандартизації, сертифікації та якості» від 23 вересня 2016 року № 279 (EN 419211-3:2013, IDT)
32. ДСТУ EN 419211-4:2016 «Профілі захисту для пристроїв створення безпечного підпису. Частина 4. Розширення для пристроїв з генерацією ключів та довіреним каналом для застосування генерації сертифікатів», затверджений наказом державного підприємства «Український науково-дослідний і навчальний центр проблем стандартизації, сертифікації та якості» від 23 вересня 2016 року № 279 (EN 419211-4:2013, IDT)
33. ДСТУ EN 419211-5:2016 «Профілі захисту для пристроїв створення безпечного підпису. Частина 5. Розширення для пристроїв з генерацією ключів та довіреним каналом для застосування створення підпису», затверджений наказом державного підприємства «Український науково-дослідний і навчальний центр проблем стандартизації, сертифікації та якості» від 23 вересня 2016 року № 279 (EN 419211-5:2013, IDT)
34. ДСТУ EN 419211-6:2016 «Профілі захисту для пристроїв створення безпечного підпису. Частина 6. Розширення для пристроїв з імпортом ключів та довіреним каналом для застосування створення підпису», затверджений наказом державного підприємства «Український науково-дослідний і навчальний центр проблем стандартизації, сертифікації та якості» від 23 вересня 2016 року № 279 (EN 419211-6:2014, IDT)
35. ДСТУ ISO/IEC 19790:2015 «Інформаційні технології. Методи захисту. Вимоги безпеки до криптографічних модулів», затверджений наказом державного підприємства «Український науково-дослідний і навчальний центр проблем стандартизації, сертифікації та якості» від 18 грудня 2015 року № 193 (ISO/IEC 19790:2012, IDT)

Стандарти, що визначають вимоги до кваліфікованих сертифікатів відкритих ключів

36. ДСТУ ETSI EN 319 412-1:2016 «Електронні підписи й інфраструктури (ESI). Профілі сертифікатів. Частина 1. Огляд та типові структури даних», затверджений наказом державного підприємства «Український науково-дослідний і навчальний центр проблем стандартизації, сертифікації та якості» від 21 червня 2016 року № 183 (ETSI EN 319 412-1:2016, IDT)
37. ДСТУ ETSI EN 319 412-2:2016 «Електронні підписи та інфраструктури. Профілі сертифікатів. Частина 2. Профілі сертифікатів, випущених для фізичних осіб», затверджений наказом державного підприємства «Український науково-дослідний і навчальний центр проблем стандартизації, сертифікації та якості» від 23 вересня 2016 року № 279 (ETSI EN 319 412-2:2016, IDT)

Продовження додатка

38. ДСТУ ETSI EN 319 412-3:2016 «Електронні підписи та інфраструктури (ESI). Профілі сертифікатів. Частина 3. Профіль сертифіката юридичної особи», затверджений наказом державного підприємства «Український науково-дослідний і навчальний центр проблем стандартизації, сертифікації та якості» від 27 грудня 2016 року № 451 (ETSI EN 319 412-3:2016, IDT)
39. ДСТУ ETSI EN 319 412-4:2016 «Електронні підписи й інфраструктури (ESI). Профілі сертифікатів. Частина 4. Профіль сертифіката для сертифікатів веб-сайтів», затверджений наказом державного підприємства «Український науково-дослідний і навчальний центр проблем стандартизації, сертифікації та якості» від 21 червня 2016 року № 183 (ETSI EN 319 412-4:2016, IDT)
40. ДСТУ ETSI EN 319 412-5:2016 «Електронні підписи та інфраструктури. Профілі сертифікатів. Частина 5. Системи контролю якості», затверджений наказом державного підприємства «Український науково-дослідний і навчальний центр проблем стандартизації, сертифікації та якості» від 23 вересня 2016 року № 279 (ETSI EN 319 412-5:2016, IDT)

Стандарти, що визначають вимоги до криптографічного захисту інформації

41. ДСТУ 4145-2002 «Інформаційні технології. Криптографічний захист інформації. Цифровий підпис, що ґрунтується на еліптичних кривих. Формування та перевіряння», затверджений наказом Державного комітету України з питань технічного регулювання та споживчої політики від 28 грудня 2002 року № 31
42. ДСТУ 7564:2014 «Інформаційні технології. Криптографічний захист інформації. Функція ґешування», затверджений наказом Міністерства економічного розвитку і торгівлі України від 02 грудня 2014 року № 1431
43. ДСТУ 7624:2014 «Інформаційні технології. Криптографічний захист інформації. Алгоритм симетричного блокового перетворення», затверджений наказом Міністерства економічного розвитку і торгівлі України від 29 грудня 2014 року № 1484
44. ДСТУ ETSI TR 119 300:2016 «Електронні підписи та інфраструктури (ESI). Настанова щодо застосування стандартів для криптографічних комплектів», затверджений наказом державного підприємства «Український науково-дослідний і навчальний центр проблем стандартизації, сертифікації та якості» від 27 грудня 2016 року № 451 (ETSI TR 119 300:2016, IDT)

Продовження додатка

45. ДСТУ ETSI TS 119 312:2015 «Електронні підписи й інфраструктури (ESI). Криптографічні комплекти», затверджений наказом державного підприємства «Український науково-дослідний і навчальний центр проблем стандартизації, сертифікації та якості» від 05 листопада 2015 року № 145 (ETSI TS 119 312:2014, IDT)
46. ДСТУ ETSI TR 102 272:2015 «Електронні підписи та інфраструктура (ESI). ASN.1 формат політики підпису», затверджений наказом державного підприємства «Український науково-дослідний і навчальний центр проблем стандартизації, сертифікації та якості» від 27 листопада 2015 року № 164 (ETSI TR 102 272:2003, IDT)
47. ДСТУ ETSI TS 102 176-1:2017 «Електронні підписи та інфраструктури (ESI). Алгоритми та параметри безпечних електронних підписів. Частина 1. Геш-функції й асиметричні алгоритми», затверджений наказом державного підприємства «Український науково-дослідний і навчальний центр проблем стандартизації, сертифікації та якості» від 09 серпня 2017 року № 214 (ETSI TS 102 176-1:2011, IDT)
48. ДСТУ ISO/IEC 14888-1:2015 «Інформаційні технології. Методи захисту. Цифрові підписи з доповненням. Частина 1. Загальні положення», затверджений наказом державного підприємства «Український науково-дослідний і навчальний центр проблем стандартизації, сертифікації та якості» від 18 грудня 2015 року № 193 (ISO/IEC 14888-1:2008, IDT)
49. ДСТУ ISO/IEC 14888-2:2015 «Інформаційні технології. Методи захисту. Цифрові підписи з доповненням. Частина 2. Механізми, що ґрунтуються на факторизації цілих чисел», затверджений наказом державного підприємства «Український науково-дослідний і навчальний центр проблем стандартизації, сертифікації та якості» від 18 грудня 2015 року № 193 (ISO/IEC 14888-2:2008, IDT)
50. ДСТУ ISO/IEC 14888-3:2015 «Інформаційні технології. Методи захисту. Цифрові підписи з доповненням. Частина 3. Механізми, що ґрунтуються на дискретному логарифмуванні», затверджений наказом державного підприємства «Український науково-дослідний і навчальний центр проблем стандартизації, сертифікації та якості» від 18 грудня 2015 року № 193 (ISO/IEC 4888-3:2006; Cor 1:2007; Cor 2:2009; Amd 1:2010; Amd 2:2012, IDT)

Стандарти, що визначають вимоги до інформаційної безпеки

51. ДСТУ ISO/IEC 18045:2015 «Інформаційні технології. Методи захисту. Методологія оцінювання безпеки ІТ», затверджений наказом державного підприємства «Український науково-дослідний і навчальний центр проблем стандартизації, сертифікації та якості» від 18 грудня 2015 року № 193 (ISO/IEC 18045:2008, IDT)

Продовження додатка

52. ДСТУ ISO/IEC 15408-1:2017 «Інформаційні технології. Методи захисту. Критерії оцінки. Частина 1. Вступ та загальна модель», затверджений наказом державного підприємства «Український науково-дослідний і навчальний центр проблем стандартизації, сертифікації та якості» від 04 серпня 2017 року № 207 (ISO/IEC 15408-1:2009, IDT)
53. ДСТУ ISO/IEC 15408-2:2017 «Інформаційні технології. Методи захисту. Критерії оцінки. Частина 2. Функціональні вимоги», затверджений наказом державного підприємства «Український науково-дослідний і навчальний центр проблем стандартизації, сертифікації та якості» від 04 серпня 2017 року № 207 (ISO/IEC 15408-2:2008, IDT)
54. ДСТУ ISO/IEC 15408-3:2017 «Інформаційні технології. Методи захисту. Критерії оцінки. Частина 3. Вимоги до гарантії безпеки», затверджений наказом державного підприємства «Український науково-дослідний і навчальний центр проблем стандартизації, сертифікації та якості» від 04 серпня 2017 року № 207 (ISO/IEC 15408-3:2008, IDT)
55. ДСТУ ISO/IEC 27001:2015 «Інформаційні технології. Методи захисту. Системи управління інформаційною безпекою. Вимоги», затверджений наказом державного підприємства «Український науково-дослідний і навчальний центр проблем стандартизації, сертифікації та якості» від 18 грудня 2015 року № 193 (ISO/IEC 27001:2013; Cor 1:2014, IDT)
56. ДСТУ ISO/IEC 27002:2015 «Інформаційні технології. Методи захисту. Звід практик щодо заходів інформаційної безпеки», затверджений наказом державного підприємства «Український науково-дослідний і навчальний центр проблем стандартизації, сертифікації та якості» від 18 грудня 2015 року № 193 (ISO/IEC 27002:2013; Cor 1:2014, IDT)
57. ДСТУ ISO/IEC 27005:2015 «Інформаційні технології. Методи захисту. Управління ризиками інформаційної безпеки», затверджений наказом державного підприємства «Український науково-дослідний і навчальний центр проблем стандартизації, сертифікації та якості» від 18 грудня 2015 року № 193 (ISO/IEC 27005:2011, IDT)

Стандарти щодо тестування інтероперабельності

58. ДСТУ ETSI SR 003 186:2017 «Електронні підписи та інфраструктури (ESI). Тестування інтероперабельності та заходи, необхідні для імплементації та популяризації моделі цифрових підписів», затверджений наказом державного підприємства «Український науково-дослідний і навчальний центр проблем стандартизації, сертифікації та якості» від 04 серпня 2017 року № 206 (ETSI SR 003 186:2016, IDT)

2) новий список відкликаних сертифікатів може бути опублікований до настання граничного терміну його дії до видання наступного списку;

3) на список відкликаних сертифікатів повинен бути накладений кваліфікований електронний підпис чи печатка надавача.

46. Управління статусом кваліфікованого сертифіката електронного підпису чи печатки та розповсюдження інформації про статус кваліфікованого сертифіката електронного підпису чи печатки повинні бути доступні користувачу цілодобово.

47. Заяви про скасування або блокування кваліфікованого сертифіката електронного підпису чи печатки фіксуються та зберігаються надавачем протягом строків, визначених законодавством.

48. Надавач повинен забезпечити цілісність та походження інформації про статус кваліфікованих сертифікатів електронного підпису чи печатки.

49. Час, що використовується надавачем в процесі обслуговування кваліфікованих сертифікатів електронного підпису чи печатки користувачів, повинен бути синхронізований з Всесвітнім координованим часом (UTC) з точністю до секунди.

50. Формування кваліфікованого сертифіката електронного підпису чи печатки здійснюється надавачем за запитом користувача.

51. Надавачі отримують кваліфіковану електронну довірчу послугу формування, перевірки та підтвердження чинності кваліфікованого сертифіката електронного підпису чи печатки від центрального засвідчувального органу.

4. Вимоги до надання кваліфікованої електронної довірчої послуги формування, перевірки та підтвердження чинності кваліфікованого сертифіката автентифікації веб-сайту

52. Кваліфікована електронна довірча послуга формування, перевірки та підтвердження чинності кваліфікованого сертифіката автентифікації веб-сайту включає вчинення дій, передбачених частиною першою статті 21 Закону України «Про електронні довірчі послуги».

53. Формування кваліфікованого сертифіката автентифікації веб-сайту здійснюється надавачем за запитом користувача.

54. Кваліфікований сертифікат автентифікації веб-сайту повинен забезпечувати:

1) автентифікацію власника веб-сайту;

2) гарантування:

шифрування інформації, обмін якою здійснюють через Інтернет учасник он-лайн операції та веб-сайт;

належного рівня довіри до власника веб-сайту щодо захисту від шахрайства в Інтернеті;

захисту особистої інформації та персональних даних учасника он-лайн операції під час вчинення такої операцій.

55. Перевірка кваліфікованого сертифіката автентифікації веб-сайту може здійснюватися будь-якою особою з метою отримання інформації про власника веб-сайту та чинність кваліфікованого сертифіката автентифікації веб-сайту.

56. Під час перевірки кваліфікованого сертифіката автентифікації веб-сайту особа, що здійснює перевірку, виконує такі дії:

1) отримує з кваліфікованого сертифіката автентифікації веб-сайту інформацію, що містить ідентифікаційні дані особи, які дають змогу однозначно встановити власника веб-сайту та надавача;

2) перевіряє кваліфікований електронний підпис чи печатку, накладений на кваліфікований сертифікат автентифікації веб-сайту за допомогою чинного (на момент формування кваліфікованого сертифіката автентифікації веб-сайту) кваліфікованого сертифіката відкритого ключа надавача.

57. Кваліфікований сертифікат автентифікації веб-сайту вважається нечинним у разі:

1) закінчення строку дії кваліфікованого сертифіката автентифікації веб-сайту або зміни його статусу на блокований чи скасований;

2) використання скасованого або блокованого кваліфікованого сертифіката відкритого ключа надавача на момент формування кваліфікованого сертифіката автентифікації веб-сайту.

58. Надавачі отримують кваліфіковану електронну довірчу послугу формування, перевірки та підтвердження чинності кваліфікованого сертифіката автентифікації веб-сайту від центрального засвідчувального органу.

5. Вимоги до надання кваліфікованої електронної довірчої послуги формування, перевірки та підтвердження кваліфікованої електронної позначки часу

59. Кваліфікована електронна довірча послуга формування, перевірки та підтвердження кваліфікованої електронної позначки часу включає вчинення дій, передбачених частиною першою статті 26 Закону України «Про електронні довірчі послуги».

60. Формування кваліфікованої електронної позначки часу здійснюється надавачем за запитом користувача.

61. Під час формування кваліфікованої електронної позначки часу користувач та надавач за допомогою засобів кваліфікованого електронного підпису чи печатки виконують такі дії:

1) користувач обчислює геш-значення електронних даних, на які необхідно сформувати кваліфіковану електронну позначку часу;

2) користувач формує запит на формування кваліфікованої електронної позначки часу, який містить:

обчислене геш-значення;

об'єктний ідентифікатор політики формування позначки часу (необов'язково);

ідентифікатор алгоритму гешування, що використовувався;

унікальний ідентифікатор запиту (необов'язково);

необов'язкові розширення;

3) користувач передає сформований запит до надавача;

4) надавач перевіряє правильність формату запиту та виконує його обробку, формує кваліфіковану електронну позначку часу та відповідь, що містить кваліфіковану електронну позначку часу, чи відповідь з інформацією про відмову у формуванні кваліфікованої електронної позначки часу;

5) надавач пересилає користувачеві відповідь, що містить кваліфіковану електронну позначку часу, яка містить такі дані:

об'єктний ідентифікатор політики формування кваліфікованої електронної позначки часу, що була використана;

геш-значення електронних даних, для яких було сформовано кваліфіковану електронну позначку часу;

серійний номер кваліфікованої електронної позначки часу;

час формування кваліфікованої електронної позначки часу;

додаткову інформацію про кваліфіковану електронну позначку часу;

кваліфікований електронний підпис чи печатку надавача, накладений на кваліфіковану електронну позначку часу;

6) користувач після отримання відповіді від надавача виконує такі дії:

перевіряє результат обробки у відповіді;

перевіряє відповідність імені чи найменування суб'єкта, що наклав кваліфікований електронний підпис чи печатку на кваліфіковану електронну позначку часу, імені чи найменуванню надавача;

перевіряє відповідність призначення кваліфікованого сертифіката відкритого ключа надавача (для формування позначки часу);

перевіряє чинність кваліфікованого сертифіката відкритого ключа надавача;

перевіряє кваліфікований електронний підпис чи печатку, що був накладений на кваліфіковану електронну позначку часу;

перевіряє відповідність електронних даних та даних, для яких була сформована кваліфікована електронна позначка часу (шляхом порівняння обчисленого геш-значення електронних даних та геш-значення, що записане у кваліфікованій електронній позначці часу);

додає кваліфіковану електронну позначку часу до електронних даних.

62. Кваліфікована електронна позначка часу повинна забезпечувати:

1) зв'язок дати і часу з електронними даними в такий спосіб, що цілком виключає можливість непомітної зміни електронних даних;

2) точність часу в програмно-технічному комплексі надавача, що синхронізується із Всесвітнім координованим часом (UTC) з точністю до секунди.

63. Перевірка кваліфікованої електронної позначки часу може здійснюватися будь-якою особою з метою отримання інформації про чинність кваліфікованої електронної позначки часу.

64. Під час перевірки та підтвердження кваліфікованої електронної позначки часу особа, що здійснює перевірку, виконує такі дії:

1) отримує з кваліфікованої електронної позначки часу інформацію, що містить ідентифікаційні дані особи, які дають змогу однозначно встановити надавача;

2) перевіряє кваліфікований електронний підпис чи печатку, накладений на кваліфіковану електронну позначку часу за допомогою чинного (на момент формування кваліфікованої електронної позначки часу) кваліфікованого сертифіката відкритого ключа надавача;

3) перевіряє відповідність кваліфікованої електронної позначки часу та електронних даних, до яких вона додана (шляхом порівняння обчисленого геш-значення електронних даних та геш-значення, що записане у кваліфікованій електронній позначці часу).

65. Кваліфікована електронна позначка часу вважається недійсною у разі:

1) недотримання вимоги щодо точності часу в програмно-технічному комплексі надавача;

2) використання скасованого або блокованого кваліфікованого сертифіката відкритого ключа надавача на момент формування кваліфікованої електронної позначки часу.

66. Правильність реалізації криптографічних алгоритмів для створення кваліфікованої електронної позначки часу та точність часу в засобі

кваліфікованого електронного підпису чи печатки забезпечує протокол фіксування часу.

67. Надавачі отримують кваліфіковану електронну довірчу послугу формування, перевірки та підтвердження кваліфікованої електронної позначки часу від центрального засвідчувального органу.

68. Механізм синхронізації часу із Всесвітнім координованим часом (UTC) в програмно-технічному комплексі надавача та склад технічного обладнання, що застосовується у процесі синхронізації часу (його загальний опис) встановлюється Порядком синхронізації часу із Всесвітнім координованим часом (UTC).

Порядок синхронізації часу із Всесвітнім координованим часом (UTC) розробляється надавачем та погоджується з центральним засвідчувальним органом.

6. Вимоги до надання кваліфікованої електронної довірчої послуги реєстрованої електронної доставки

69. Кваліфікована електронна довірча послуга реєстрованої електронної доставки повинна відповідати вимогам, передбаченим частиною першою статті 27 Закону України «Про електронні довірчі послуги», та включати вчинення таких дій:

1) відправку електронних даних із забезпеченням доказів відправки;

2) отримання електронних даних із забезпеченням доказів отримання.

70. Реєстрована електронна доставка здійснюється надавачем за запитом користувача (відправника та/або отримувача електронних даних).

71. Реєстрована електронна доставка повинна забезпечувати:

1) передачу електронних даних між користувачами (відправником та отримувачем електронних даних);

2) автентифікацію відправника та отримувача електронних даних;

3) конфіденційність електронних даних, що доставляються, та персональних даних відправника та отримувача електронних даних;

4) захист цілісності електронних даних, що доставляються;

5) забезпечення точності дати та часу відправки та отримання електронних даних;

6) можливість доказування відправки та отримання електронних даних.

72. Перевірка електронних даних, що передаються в процесі реєстрованої електронної доставки, здійснюється отримувачем електронних даних.

7. Вимоги до надання кваліфікованої електронної довірчої послуги зберігання кваліфікованих електронних підписів, печаток, електронних позначок часу та сертифікатів, пов'язаних з цими послугами

73. Кваліфікована електронна довірча послуга зберігання кваліфікованих електронних підписів, печаток, електронних позначок часу та сертифікатів, пов'язаних з цими послугами, включає вчинення таких дій:

1) передачу кваліфікованих електронних підписів чи печаток, позначок часу та сформованих сертифікатів, пов'язаних з цими послугами;

2) зберігання кваліфікованих електронних підписів чи печаток, позначок часу та сформованих сертифікатів, пов'язаних з цими послугами.

74. Зберігання кваліфікованих електронних підписів, печаток, електронних позначок часу та сертифікатів, пов'язаних з цими послугами, здійснюється надавачем за запитом користувача.

75. При наданні електронної довірчої послуги зберігання кваліфікованих електронних підписів, печаток, електронних позначок часу та сертифікатів повинно забезпечуватися:

1) цілісність всіх збережених об'єктів даних;

2) протоколювання подій на предмет зміни, видалення або додавання об'єктів даних;

3) покладання відповідальності за збереження на одну чи декількох конкретних посадових осіб;

4) проведення регулярних перевірок дотримання цих Вимог.

III. Вимоги до засобів кваліфікованого електронного підпису чи печатки

1. Засоби кваліфікованого електронного підпису чи печатки, що використовуються під час надання кваліфікованих електронних довірчих послуг, повинні відповідати вимогам, встановленим частинами першою та другою статті 19 Закону України «Про електронні довірчі послуги».

2. Для надання кваліфікованих електронних довірчих послуг використовуються засоби кваліфікованого електронного підпису чи печатки, які повинні мати документи про відповідність або позитивний експертний висновок за результатами їх державної експертизи у сфері криптографічного захисту інформації.

3. Надання кваліфікованих електронних довірчих послуг надавачем без чинних документів, що підтверджують його право власності та/або право користування засобами кваліфікованого електронного підпису чи печатки, які

використовуються для надання кваліфікованих електронних довірчих послуг, забороняється.

4. Технічні специфікації форматів, які реалізуються у засобах кваліфікованого електронного підпису чи печатки, встановлюються головним органом у системі центральних органів виконавчої влади, що забезпечує формування та реалізує державну політику у сфері електронних довірчих послуг, спільно з спеціально уповноваженим центральним органом виконавчої влади з питань організації спеціального зв'язку та захисту інформації.

5. Контроль за дотриманням вимог до засобів кваліфікованого електронного підпису чи печатки здійснює контролюючий орган.

IV. Вимоги до кваліфікованих сертифікатів відкритих ключів

1. Кваліфіковані сертифікати відкритих ключів, що формуються надавачами або центральним засвідчувальним органом під час надання кваліфікованих електронних довірчих послуг, повинні відповідати вимогам, встановленим частинами першою, другою та третьою статті 23 Закону України «Про електронні довірчі послуги».

2. Надавач або центральний засвідчувальний орган, який видав кваліфікований сертифікат відкритого ключа, повинен забезпечити доступ до інформації про дату та час зміни статусу кваліфікованого сертифіката відкритого ключа.

3. Контроль за дотриманням вимог до кваліфікованих сертифікатів відкритих ключів здійснює контролюючий орган.

Додаток
до Вимог у сфері електронних довірчих послуг

ПЕРЕЛІК СТАНДАРТІВ,
що застосовуються кваліфікованими надавачами електронних довірчих послуг під час надання кваліфікованих електронних довірчих послуг

№ з/п	Назва стандарту
	Стандарти, що визначають загальні вимоги до кваліфікованого надавача електронних довірчих послуг під час надання кваліфікованих електронних довірчих послуг
1.	ДСТУ ETSI TR 119 400:2017 «Електронні підписи та інфраструктури (ESI). Настанова з використання стандартів провайдерами довірчих послуг, які підтримують цифрові підписи та пов'язані з ними послуги», затверджений наказом державного підприємства «Український науково-дослідний і навчальний центр проблем стандартизації, сертифікації та якості» від 04 серпня 2017 року № 207 (ETSI TR 119 400:2016, IDT)
2.	ДСТУ ETSI EN 319 401:2016 «Електронні підписи й інфраструктури (ESI). Загальні вимоги політики для провайдерів довірчих послуг», затверджений наказом державного підприємства «Український науково-дослідний і навчальний центр проблем стандартизації, сертифікації та якості» від 21 червня 2016 року № 183 (ETSI EN 319 401:2016, IDT)
3.	ДСТУ ETSI EN 319 403:2016 «Електронні підписи та інфраструктури (ESI). Оцінювання відповідності провайдерів довірчих послуг. Вимоги до органів з оцінювання відповідності, що оцінюють провайдерів довірчих послуг», затверджений наказом державного підприємства «Український науково-дослідний і навчальний центр проблем стандартизації, сертифікації та якості» від 27 грудня 2016 року № 451 (ETSI EN 319 403:2015, IDT)
	Стандарти, що визначають вимоги до Довірчого списку
4.	ДСТУ ETSI TR 119 600:2016 «Електронні підписи та інфраструктури (ESI). Настанова щодо застосування стандартів для провайдерів переліків стану довірчих послуг», затверджений наказом державного підприємства «Український науково-дослідний і навчальний центр проблем стандартизації, сертифікації та якості» від 27 грудня 2016 року № 451 (ETSI TR 119 600:2016, IDT)
5.	ДСТУ ETSI TS 119 612:2016 «Електронні підписи та інфраструктури. Довірчі списки», затверджений наказом державного підприємства «Український науково-дослідний і навчальний центр проблем стандартизації, сертифікації та якості» від 23 вересня 2016 року № 279 (ETSI TS 119 612:2016, IDT)

Продовження додатка

59. ДСТУ ETSI TS 119 124-4:2017 «Електронні підписи та інфраструктури (ESI). Цифрові підписи CAdES. Перевірка на відповідність і інтероперабельність. Частина 4. Тестування на відповідність базових підписів CAdES», затверджений наказом державного підприємства «Український науково-дослідний і навчальний центр проблем стандартизації, сертифікації та якості» від 04 серпня 2017 року № 207 (ETSI TS 119 124-4:2016, IDT)
60. ДСТУ ETSI TR 119 134-1:2017 «Електронні підписи та інфраструктури (ESI). Цифрові підписи XAdES. Тестування на відповідність та інтероперабельність. Частина 1. Огляд», затверджений наказом державного підприємства «Український науково-дослідний і навчальний центр проблем стандартизації, сертифікації та якості» від 30 листопада 2017 року № 392 (ETSI TR 119 134-1:2016, IDT)
61. ДСТУ ETSI TR 119 134-2:2017 «Електронні підписи та інфраструктури (ESI). Цифрові підписи XAdES. Тестування на відповідність та інтероперабельність. Частина 2. Набори тестів для тестування інтероперабельності базових підписів XAdES», затверджений наказом державного підприємства «Український науково-дослідний і навчальний центр проблем стандартизації, сертифікації та якості» від 30 листопада 2017 року № 392 (ETSI TR 119 134-2:2016, IDT)
62. ДСТУ ETSI TR 119 134-3:2017 «Електронні підписи та інфраструктури (ESI). Цифрові підписи XAdES. Тестування на відповідність та інтероперабельність. Частина 3. Набори тестів для тестування інтероперабельності посилених підписів XAdES», затверджений наказом державного підприємства «Український науково-дослідний і навчальний центр проблем стандартизації, сертифікації та якості» від 30 листопада 2017 року № 392 (ETSI TR 119 134-3:2016, IDT)
63. ДСТУ ETSI TR 119 134-4:2017 «Електронні підписи та інфраструктури (ESI). Цифрові підписи XAdES. Тестування на відповідність та інтероперабельність. Частина 4. Тестування на відповідність базовим підписам XAdES», затверджений наказом державного підприємства «Український науково-дослідний і навчальний центр проблем стандартизації, сертифікації та якості» від 30 листопада 2017 року № 392 (ETSI TR 119 134-4:2016, IDT)
64. ДСТУ ETSI TR 119 134-5:2017 «Електронні підписи та інфраструктури (ESI). Цифрові підписи XAdES. Тестування на відповідність та інтероперабельність. Частина 5. Тестування на відповідність посилених підписів XAdES», затверджений наказом державного підприємства «Український науково-дослідний і навчальний центр проблем стандартизації, сертифікації та якості» від 30 листопада 2017 року № 392 (ETSI TR 119 134-5:2016, IDT)

Продовження додатка

65. ДСТУ ETSI TR 119 144-1:2017 «Електронні підписи та інфраструктури (ESI). Цифрові підписи PAdES. Тестування відповідності та інтероперабельності. Частина 1. Огляд», затверджений наказом державного підприємства «Український науково-дослідний і навчальний центр проблем стандартизації, сертифікації та якості» від 04 серпня 2017 року № 207 (ETSI TR 119 144-1:2016, IDT)
66. ДСТУ ETSI TS 119 144-2:2017 «Електронні підписи та інфраструктури (ESI). Цифрові підписи PAdES. Тестування відповідності та інтероперабельності. Частина 2. Набори тестів для тестування інтероперабельності базових підписів PAdES», затверджений наказом державного підприємства «Український науково-дослідний і навчальний центр проблем стандартизації, сертифікації та якості» від 04 серпня 2017 року № 207 (ETSI TS 119 144-2:2016, IDT)
67. ДСТУ ETSI TS 119 144-3:2017 «Електронні підписи та інфраструктури (ESI). Цифрові підписи PAdES. Тестування відповідності та інтероперабельності. Частина 3. Набори тестів для тестування інтероперабельності додаткових підписів PAdES», затверджений наказом державного підприємства «Український науково-дослідний і навчальний центр проблем стандартизації, сертифікації та якості» від 04 серпня 2017 року № 207 (ETSI TS 119 144-3:2016, IDT)
68. ДСТУ ETSI TS 119 144-4:2017 «Електронні підписи та інфраструктури (ESI). Цифрові підписи PAdES. Тестування відповідності та інтероперабельності. Частина 4. Тестування відповідності базових підписів PAdES», затверджений наказом державного підприємства «Український науково-дослідний і навчальний центр проблем стандартизації, сертифікації та якості» від 04 серпня 2017 року № 207 (ETSI TS 119 144-4:2016, IDT)
69. ДСТУ ETSI TS 119 144-5:2017 «Електронні підписи та інфраструктури (ESI). Цифрові підписи PAdES. Тестування відповідності та інтероперабельності. Частина 5. Тестування відповідності додаткових підписів PAdES», затверджений наказом державного підприємства «Український науково-дослідний і навчальний центр проблем стандартизації, сертифікації та якості» від 04 серпня 2017 року № 207 (ETSI TS 119 144-5:2016, IDT)

ЗАТВЕРДЖЕНО
постановою Кабінету Міністрів України
від 2018 р. №

ПОРЯДОК
перевірки дотримання вимог законодавства у сфері електронних довірчих послуг

Розділ І. Загальні положення

1. Сфера дії

1. Порядок перевірки дотримання вимог законодавства у сфері електронних довірчих послуг визначає механізм проведення контролюючим органом заходів державного нагляду (контролю) за дотриманням вимог законодавства у сфері електронних довірчих послуг, у тому числі обов'язкових умов, яких повинні дотримуватись кваліфіковані надавачі електронних довірчих послуг (далі – надавачі), їх відокремлені пункти реєстрації під час надання кваліфікованих електронних довірчих послуг.

2. Державний нагляд (контроль) за дотриманням вимог законодавства у сфері електронних довірчих послуг центральним засвідчувальним органом здійснюється контролюючим органом відповідно до цього Порядку з урахуванням особливостей, передбачених законодавством.

3. Дія цього Порядку не поширюється на засвідчувальний центр та надавачів, внесених до Довірчого списку за поданням засвідчувального центру, та їх відокремлені пункти реєстрації.

2. Визначення термінів

4. Терміни, що вживаються в цьому Порядку, мають таке значення:

безвиїзний нагляд – захід державного нагляду (контролю) за дотриманням вимог законодавства у сфері електронних довірчих послуг, що здійснюється посадовими особами контролюючого органу без виїзду за місцезнаходженням надавача, його відокремлених пунктів реєстрації або центрального засвідчувального органу, пов'язаний зі збором інформації, з метою отримання відомостей про явища та процеси, що відбуваються під час надання кваліфікованих електронних довірчих послуг;

інформаційно-телекомунікаційна система – сукупність інформаційних та телекомунікаційних систем надавача або центрального засвідчувального органу, які у процесі обробки інформації діють як єдине ціле та об'єднують програмно-технічний комплекс, що використовується під час надання кваліфікованих електронних довірчих послуг (далі – програмно-технічний комплекс), фізичне середовище, інформацію, що обробляється в цих системах, а також найманих працівників надавача або центрального засвідчувального органу, які безпосередньо задіяні у наданні кваліфікованих електронних довірчих послуг або обслуговують програмно-технічний комплекс (далі – наймані працівники);

кваліфікована електронна довірча послуга – електронна довірча послуга, надання якої забезпечує надавач, його відокремлені пункти реєстрації або центральний засвідчувальний орган за допомогою засобу кваліфікованого електронного підпису чи печатки та базується на кваліфікованому сертифікаті відкритого ключа;

перевірка – виїзний плановий або позаплановий захід державного нагляду (контролю) за дотриманням вимог законодавства у сфері електронних довірчих послуг, що здійснюється посадовими особами контролюючого органу відповідно до їх функціональних обов'язків за місцезнаходженням надавача, його відокремлених пунктів реєстрації або центрального засвідчувального органу;

регламент роботи – нормативний документ надавача або центрального засвідчувального органу, що визначає організаційно-методологічні, технічні та технологічні умови діяльності надавача або центрального засвідчувального органу під час надання кваліфікованих електронних довірчих послуг, включаючи політику сертифіката та положення сертифікаційних практик;

спеціальні приміщення – нежилі приміщення, які використовуються надавачем або центральним засвідчувальним органом для розміщення всіх складових програмно-технічного комплексу.

5. Інші терміни вживаються у значеннях, наведених у законах України «Про електронні довірчі послуги», «Про електронні документи та електронний

документообіг», «Про основні засади державного нагляду (контролю) у сфері господарської діяльності», «Про телекомунікації», «Про захист інформації в інформаційно-телекомунікаційних системах».

3. Заходи державного нагляду (контролю) за дотриманням вимог законодавства у сфері електронних довірчих послуг

6. Заходи державного нагляду (контролю) за дотриманням вимог законодавства у сфері електронних довірчих послуг здійснюються контролюючим органом шляхом проведення безвиїзного нагляду, планових та позапланових перевірок надавачів, їх відокремлених пунктів реєстрації або центрального засвідчувального органу.

7. Основними завданнями державного нагляду (контролю) за дотриманням вимог законодавства у сфері електронних довірчих послуг є забезпечення:

1) дотримання надавачами, їх відокремленими пунктами реєстрації, центральним засвідчувальним органом вимог законодавства у сфері електронних довірчих послуг;

2) оцінки діяльності надавачів, їх відокремлених пунктів реєстрації, центрального засвідчувального органу щодо дотримання вимог законодавства у сфері електронних довірчих послуг;

3) своєчасного попередження, виявлення та припинення дій або бездіяльності надавачів, їх відокремлених пунктів реєстрації, центрального засвідчувального органу, які містять ознаки порушення вимог законодавства у сфері електронних довірчих послуг;

4) усунення причин виникнення порушень вимог законодавства у сфері електронних довірчих послуг і умов, що їм сприяють;

5) вжиття заходів для усунення наслідків порушень вимог законодавства у сфері електронних довірчих послуг після їх припинення та притягнення винних осіб до відповідальності.

8. Державний нагляд (контроль) за дотриманням вимог законодавства у сфері електронних довірчих послуг реалізується контролюючим органом шляхом здійснення:

1) перевірок надавачів, їх відокремлених пунктів реєстрації або центрального засвідчувального органу;

2) аналізу звітів про діяльність надавачів, наданих ними відповідно до вимог законодавства у сфері електронних довірчих послуг;

3) опрацювання інформації чи повідомлень про порушення надавачем вимог законодавства у сфері електронних довірчих послуг;

4) погодження регламентів роботи надавачів, центрального засвідчувального органу;

5) аналізу стану дотримання порядку використання електронних довірчих послуг в органах державної влади, органах місцевого самоврядування, підприємствах, установах та організаціях державної форми власності;

6) взаємодії з центральним засвідчувальним органом та органами з оцінки відповідності з питань державного нагляду (контролю) за дотриманням вимог законодавства у сфері електронних довірчих послуг;

7) співпраці з органами з питань захисту персональних даних шляхом інформування про порушення законодавства у сфері захисту персональних даних, виявлені під час проведення перевірок надавачів;

8) аналізу документів про відповідність за результатами проведення процедур оцінки відповідності надавачів;

9) видання приписів щодо усунення порушень вимог законодавства у сфері електронних довірчих послуг;

10) накладення адміністративних штрафів за порушення вимог законодавства у сфері електронних довірчих послуг;

11) інформування Кабінету Міністрів України у разі виявлення порушень вимог законодавства у сфері електронних довірчих послуг за результатами перевірки центрального засвідчувального органу;

12) підготовки щорічних звітів про оцінку діяльності суб'єктів відносин у сфері електронних довірчих послуг щодо дотримання вимог законодавства у сфері електронних довірчих послуг.

9. Аналіз стану дотримання порядку використання електронних довірчих послуг в органах державної влади, органах місцевого самоврядування, підприємствах, установах та організаціях державної форми власності здійснюється контролюючим органом в рамках заходів державного нагляду (контролю) за дотриманням вимог законодавства у сфері криптографічного та технічного захисту інформації.

10. Безвиїзний нагляд проводиться контролюючим органом шляхом аналізу:

1) стану роботи офіційного веб-сайту надавача або центрального засвідчувального органу;

2) наповненості офіційного веб-сайту надавача або щодо належного інформування користувачів електронних довірчих послуг;

3) відповідності вимогам законодавства у сфері електронних довірчих послуг змісту кваліфікованих сертифікатів відкритих ключів, що формуються надавачем або центральним засвідчувальним органом;

4) переліку та порядку надання електронних довірчих послуг через офіційний веб-сайт надавача або центрального засвідчувального органу;

5) звіту про діяльність надавача, наданого ним відповідно до вимог законодавства у сфері електронних довірчих послуг;

6) іншої інформації щодо функціонування, організації та надання електронних довірчих послуг надавачем або центральним засвідчувальним органом.

11. Залежно від ступеня ризику від провадження діяльності з надання електронних довірчих послуг спеціально уповноважений центральний орган виконавчої влади з питань організації спеціального зв'язку та захисту інформації визначає періодичність проведення перевірок контролюючим органом.

Критерії, за якими оцінюється ступінь ризику від провадження діяльності з надання електронних довірчих послуг та визначається періодичність проведення контролюючим органом планових перевірок, затверджуються Кабінетом Міністрів України за поданням контролюючого органу.

Перелік питань для здійснення контролюючим органом планових перевірок залежно від ступеня ризику визначається спеціально уповноваженим центральним органом виконавчої влади з питань організації спеціального зв'язку та захисту інформації.

Планові перевірки центрального засвідчувального органу здійснюються контролюючим органом щорічно.

12. Підставами для проведення планової перевірки є:

1) річний план здійснення заходів державного нагляду (контролю), затверджений спеціально уповноваженим центральним органом виконавчої влади з питань організації спеціального зв'язку та захисту інформації;

2) план здійснення комплексних заходів державного нагляду (контролю) на відповідний плановий період, затверджений центральним органом виконавчої влади, що реалізує державну регуляторну політику, політику з питань нагляду (контролю) у сфері господарської діяльності, ліцензування та дозвільної системи у сфері господарської діяльності та дерегуляції господарської діяльності.

13. Підставами для проведення позапланової перевірки є:

1) подання надавачем заяви щодо проведення перевірки дотримання вимог законодавства у сфері електронних довірчих послуг;

2) виявлення та підтвердження недостовірності даних у документах, поданих надавачем під час внесення відомостей про надавача до Довірчого списку або формування кваліфікованого сертифіката відкритого ключа надавача;

3) невиконання вимог контролюючого органу протягом строку, визначеного у приписі про усунення порушень вимог законодавства, виданого

за результатами проведення планового заходу державного нагляду (контролю) за дотриманням вимог законодавства у сфері електронних довірчих послуг;

4) отримання інформації чи повідомлення про порушення надавачем вимог законодавства у сфері електронних довірчих послуг.

14. Предметом перевірки надавача та центрального засвідчувального органу є стан дотримання ними вимог законодавства у сфері електронних довірчих послуг, а також регламентів їх роботи.

15. Звіт про діяльність надавача подається до контролюючого органу щороку до 15 січня та містить відомості про:

1) кількість укладених договорів про надання електронних довірчих послуг (окремо з фізичними та юридичними особами);

2) кількість сформованих та скасованих кваліфікованих сертифікатів відкритих ключів за звітний період із зазначенням причин скасування (у разі якщо надавач забезпечує надання кваліфікованих електронних довірчих послуг, які передбачають обслуговування кваліфікованих сертифікатів відкритих ключів);

3) факти відшкодування шкоди користувачам електронних довірчих послуг та/або третім особам внаслідок неналежного виконання надавачем своїх зобов'язань (у разі наявності);

4) факти участі надавача як позивача, відповідача або третьої сторони у судових справах з питань надання електронних довірчих послуг, предмет розгляду та прийняте рішення (у разі наявності);

5) факти порушень надавачем вимог законодавства у сфері захисту інформації під час надання електронних довірчих послуг, їх причини та заходи, вжиті для усунення таких порушень;

6) інші питання за окремими запитами контролюючого органу.

II. Проведення перевірки

1. Організація проведення перевірки

1. У разі настання однієї з підстав для проведення планової чи позапланової перевірки контролюючий орган приймає рішення щодо проведення перевірки.

Рішення щодо проведення перевірки підписується головою контролюючого органу або його заступником відповідно до розподілу функціональних обов'язків.

2. Рішення щодо проведення перевірки повинно містити:

1) найменування контролюючого органу.

2) найменування (прізвище, ім'я, по батькові) надавача або центрального засвідчувального органу;

3) місцезнаходження надавача або центрального засвідчувального органу;

4) підставу для проведення перевірки;

5) предмет перевірки;

6) дату початку та дату закінчення перевірки;

7) посадовий та персональний склад комісії з перевірки.

3. З метою забезпечення надавачів та центральний засвідчувальний орган інформацією про заходи державного нагляду (контролю) за дотриманням вимог законодавства у сфері електронних довірчих послуг контролюючий орган зобов'язаний вносити відомості до інтегрованої автоматизованої системи державного нагляду (контролю) та оприлюднювати відповідну інформацію на своєму офіційному веб-сайті.

4. Про прийняття рішення щодо проведення перевірки надавач або центральний засвідчувальний орган повідомляється не пізніше ніж за 10 робочих днів до початку перевірки шляхом надсилання (вручення) копії такого рішення рекомендованим листом та/або за допомогою електронного поштового зв'язку або вручення особисто під розписку керівнику надавача або центрального засвідчувального органу.

5. Строки проведення планової чи позапланової перевірки встановлюються контролюючим органом відповідно до вимог Закону України «Про основні засади державного нагляду (контролю) у сфері господарської діяльності».

6. Планова та позапланова перевірка здійснюються в робочий час надавача або центрального засвідчувального органу, встановлений його правилами внутрішнього трудового розпорядку.

7. Надавач має право не допускати посадових осіб контролюючого органу до здійснення планової чи позапланової перевірки в разі неодержання у строк, визначений пунктом 4 цього підрозділу, повідомлення про прийняття рішення щодо проведення перевірки.

8. Комісія з перевірки утворюється у складі голови та членів комісії з перевірки.

До складу комісії з перевірки можуть залучатися в установленому законодавством порядку представники центрального засвідчувального органу.

9. На підставі рішення щодо проведення перевірки оформляється посвідчення на проведення перевірки, яке підписується головою

контролюючого органу або його заступником відповідно до розподілу функціональних обов'язків і засвідчується печаткою.

Форма посвідчення на проведення перевірки встановлюється спеціально уповноваженим центральним органом виконавчої влади з питань організації спеціального зв'язку та захисту інформації.

10. У посвідченні на проведення перевірки зазначаються:

1) найменування контролюючого органу;

2) найменування (прізвище, ім'я, по батькові) надавача або центрального засвідчувального органу;

3) місцезнаходження надавача або центрального засвідчувального органу;

4) реквізити рішення щодо проведення перевірки;

5) персональний та посадовий склад комісії з перевірки;

6) дата початку та дата закінчення перевірки;

7) тип перевірки (планова або позапланова);

8) підстави перевірки;

9) перелік питань, що підлягають перевірці;

10) інформація про здійснення попередньої перевірки (тип перевірки і строк її проведення).

11. Посвідчення на проведення перевірки є чинним лише протягом зазначеного в ньому строку здійснення перевірки.

2. Права та обов'язки комісії з перевірки

12. Голова комісії з перевірки зобов'язаний:

1) забезпечити координацію роботи між членами комісії з перевірки при підготовці та проведенні перевірки;

2) організувати роботу комісії з перевірки, у тому числі визначити конкретні строки, види, обсяги робіт, що потрібні для проведення перевірки;

3) здійснити розподіл питань, за якими проводиться перевірка, між членами комісії з перевірки, встановити порядок і режим їх роботи;

4) контролювати виконання доручених ним завдань.

13. Голова комісії з перевірки має право:

1) встановлювати для членів комісії з перевірки додаткові завдання з перевірки та здійснювати перерозподіл їх обов'язків;

2) здійснювати особисто перевірку будь-якої діяльності надавача або центрального засвідчувального органу, пов'язаної з наданням кваліфікованих електронних довірчих послуг;

3) запитувати у користувачів електронних довірчих послуг, які обслуговуються надавачем або центральним засвідчувальним органом, що перевіряється, відомості, які необхідні для встановлення фактичних обставин, що призвели (можуть призвести) до порушень вимог законодавства у сфері електронних довірчих послуг;

4) давати вказівки щодо оформлення акта перевірки та припису про усунення порушень;

5) давати інші вказівки щодо проведення перевірки.

14. Члени комісії з перевірки беруть участь у роботі комісії з перевірки та виконують поставлені перед ними завдання.

Член комісії з перевірки має право одноособово, керуючись конкретним завданням голови комісії з перевірки, досліджувати окремі питання перевірки.

15. Члени комісії з перевірки зобов'язані:

1) повно, об'єктивно та неупереджено здійснювати перевірку;

2) дотримуватися вимог законодавства у сферах електронних довірчих послуг, захисту інформації та захисту персональних даних;

3) сумлінно, вчасно та якісно виконувати свої службові обов'язки та доручення голови комісії з перевірки;

4) дотримуватися ділової етики у взаємовідносинах із керівником та найманими працівниками надавача або центрального засвідчувального органу;

5) ознайомити керівника надавача або центрального засвідчувального органу чи уповноваженого ним представника з результатами перевірки;

6) надавати надавачу або центральному засвідчувальному органу консультаційну допомогу щодо здійснення перевірки;

7) не розголошувати комерційну таємницю та конфіденційну інформацію, яка стала їм відома у зв'язку з виконанням службових обов'язків.

16. Члени комісії з перевірки при виконанні своїх службових обов'язків під час проведення перевірки мають право:

1) доступу до спеціальних приміщень, всіх документів та інформації надавача або центрального засвідчувального органу, пов'язаних з наданням кваліфікованих електронних довірчих послуг;

2) вивчати роботу інформаційно-телекомунікаційної системи, а також інших технічних засобів, які використовуються надавачем або центральним засвідчувальним органом для надання кваліфікованих електронних довірчих послуг;

3) одержувати від найманих працівників надавача або центрального засвідчувального органу інформацію та пояснення (у тому числі письмові) щодо їх діяльності, пов'язаної з наданням кваліфікованих електронних довірчих послуг, необхідні для здійснення перевірки;

4) отримувати від надавача або центрального засвідчувального органу та долучати до матеріалів перевірки копії документів, у тому числі виготовлені методом сканування або створення фотокопій, що можуть свідчити про факти порушення вимог законодавства у сфері електронних довірчих послуг.

17. Голова та члени комісії з перевірки відповідають згідно з законодавством за:

1) необ'єктивне відображення в акті перевірки даних про діяльність надавача або центрального засвідчувального органу;

2) приховування фактів порушень чи зловживань, виявлених під час перевірки;

3) інші дії, вчинені в процесі перевірки, які порушують вимоги законодавства.

3. Права та обов'язки надавача під час перевірки

18. Керівник надавача або центрального засвідчувального органу зобов'язаний створити необхідні умови для проведення перевірки, а саме:

1) забезпечити на період проведення перевірки голові та членам комісії з перевірки вхід до/вихід із спеціальних приміщень надавача або центрального засвідчувального органу;

2) надати голові та членам комісії з перевірки у день початку перевірки службове приміщення (окреме робоче місце), яке обладнане необхідними меблями, комп'ютером та сховищем для документів;

3) організувати зустріч голови та членів комісії з перевірки з найманими працівниками надавача або центрального засвідчувального органу, обов'язки яких безпосередньо пов'язані з наданням кваліфікованих електронних довірчих послуг;

4) забезпечити голові та членам комісії з перевірки доступ до всіх документів та інформації про діяльність надавача або центрального засвідчувального органу, пов'язану з наданням кваліфікованих електронних довірчих послуг;

5) забезпечити надання в установлені комісією з перевірки терміни документів, їх засвідчених копій та інформації про діяльність надавача або центрального засвідчувального органу (усних та письмових пояснень керівника та найманих працівників надавача або центрального засвідчувального органу);

6) забезпечувати коректну поведінку найманих працівників надавача або центрального засвідчувального органу під час проведення перевірки.

19. Вхід до службового приміщення, обладнаного для роботи комісії з перевірки, сторонніх осіб без дозволу голови комісії з перевірки забороняється.

20. Керівник надавача або центрального засвідчувального органу чи уповноважений ним представник під час проведення перевірки має право:

1) вимагати від голови та членів комісії з перевірки дотримання вимог законодавства;

2) перевіряти наявність у голови та членів комісії з перевірки службових посвідчень і одержувати копії посвідчення на проведення перевірки;

3) не допускати голови та членів комісії з перевірки до здійснення перевірки, якщо:

перевірка здійснюється з порушенням вимог щодо періодичності проведення перевірок, передбачених законодавством;

головою та членами комісії з перевірки не пред'явлено службові посвідчення та посвідчення на проведення перевірки, складеного відповідно до вимог законодавства;

4) бути присутнім під час здійснення перевірки;

5) вимагати нерозголошення комерційної таємниці та конфіденційної інформації надавача або центрального засвідчувального органу;

6) одержувати та ознайомлюватися з актом перевірки;

7) надавати в письмовій формі свої пояснення, зауваження або заперечення до акта перевірки;

8) отримувати від голови комісії з перевірки роз'яснення щодо дій комісії з перевірки, пов'язаних з перевіркою;

9) у разі неузгодження з діями голови та/або членів комісії з перевірки подавати в письмовому вигляді скарги до контролюючого органу чи оскаржувати дії комісії з перевірки в судовому порядку;

10) отримувати консультативну допомогу від голови та членів комісії з перевірки з метою запобігання порушенням під час здійснення перевірки.

21. Перед початком перевірки голова комісії з перевірки вносить запис до відповідного журналу надавача або центрального засвідчувального органу (у разі наявності).

22. Перевірка здійснюється у присутності керівника надавача або центрального засвідчувального органу чи уповноваженого ним представника.

23. Перевірка проводиться шляхом вивчення документів, інформації, що міститься в базах даних, співбесід з найманими працівниками надавача або центрального засвідчувального органу, аналізу стану дотримання вимог

законодавства у сфері електронних довірчих послуг та внутрішніх розпорядчих документів, пов'язаних з наданням кваліфікованих електронних довірчих послуг.

24. У міру виявлення порушень вимог законодавства у сфері електронних довірчих послуг, зловживань і недоліків керівництву надавача або центрального засвідчувального органу, не чекаючи закінчення перевірки, слід уживати заходів щодо усунення виявлених порушень, зловживань і недоліків, запобігання їм надалі.

4. Етапи проведення перевірки

25. Перевірка складається з таких етапів:

1) підготовка до проведення перевірки;

2) процес перевірки;

3) оформлення результатів перевірки.

26. Підготовка до проведення перевірки здійснюється шляхом:

1) опрацювання матеріалів попередньої перевірки з метою подальшого контролю за тими напрямами роботи, за якими раніше були виявлені порушення;

2) аналізу матеріалів безвиїзного нагляду;

3) вивчення регламенту роботи надавача або центрального засвідчувального органу.

27. До прийняття рішення про проведення перевірки контролюючий орган має право письмово запитувати у надавача або центрального засвідчувального органу, матеріали та інформацію, необхідні для проведення перевірки.

Надавач або центральний засвідчувальний орган зобов'язаний надати контролюючому органу всю запитувану інформацію протягом п'ятнадцяти робочих днів з дня реєстрації відповідного запиту.

28. У період підготовки до проведення перевірки голова комісії з перевірки інформує її членів про завдання (рекомендації, вказівки) перевірки, а також проводить інструктаж щодо порядку взаємодії з найманими працівниками надавача або центрального засвідчувального органу.

29. У день початку проведення перевірки голова та члени комісії з перевірки зобов'язані пред'явити керівнику надавача або центрального засвідчувального органу чи уповноваженому ним представнику посвідчення на проведення перевірки та службові посвідчення, що встановлюють голову та членів комісії з перевірки як посадових осіб контролюючого органу, і надати копію посвідчення на проведення перевірки.

30. Голова та члени комісії з перевірки не мають права здійснювати перевірку без пред'явлення службових посвідчень та посвідчення на проведення перевірки.

III. Результати перевірки

1. Оформлення результатів перевірки

1. Результати проведення перевірки надавача оформлюються комісією з перевірки шляхом складення акта перевірки, форма якого встановлюється спеціально уповноваженим центральним органом виконавчої влади з питань організації спеціального зв'язку та захисту інформації.

2. Результати проведення перевірки центрального засвідчувального органу оформлюються комісією з перевірки шляхом складення акта перевірки у довільній формі, який містить такі відомості:

1) найменування контролюючого органу

2) персональний та посадовий склад комісії з перевірки;

3) прізвище та ініціали керівника центрального засвідчувального органу;

4) тип перевірки (планова або позапланова);

5) реквізити посвідчення на проведення перевірки;

6) дату початку та дату закінчення проведення перевірки;

7) адреса приміщень центрального засвідчувального органу, пов'язаних з наданням кваліфікованих електронних довірчих послуг, в яких проводилась перевірка;

8) результати попередньої перевірки;

9) причини невиконання встановлених вимог (у разі наявності);

10) назву та короткий зміст документів, наданих під час перевірки;

11) якісні та кількісні показники, встановлені під час перевірки, що характеризують діяльність центрального засвідчувального органу, пов'язану з наданням кваліфікованих електронних довірчих послуг;

12) виявлені під час перевірки порушення і недоліки (у разі наявності);

13) висновки за результатами перевірки;

14) факти протидії проведенню перевірки (у разі наявності);

15) рекомендації щодо усунення виявлених порушень (у разі наявності);

16) дату складання акта перевірки;

17) підписи голови та членів комісії з перевірки;

18) підпис керівника центрального засвідчувального органу чи уповноваженого ним представника, що підтверджує факт ознайомлення з актом перевірки.

3. Факти порушень, недоліків, що виявлені під час перевірки, для унеможливлення неправильного тлумачення викладаються в акті перевірки об'єктивно, детально і зрозуміло.

Порушення, викладені в акті перевірки, повинні мати посилання на конкретні структурні одиниці нормативно-правових актів, що порушені.

Довільне тлумачення положень нормативно-правових актів не допускається.

Довідкову інформацію або інформацію про порушення і недоліки, яка може бути згрупована за спільним предметом, допускається викладати в додатках до акта перевірки.

Якщо до акта перевірки додаються копії документів, то в ньому відображають цей факт із зазначенням їх найменувань і реквізитів.

4. Акт перевірки складається у двох примірниках та підписується не пізніше останнього дня перевірки головою та всіма членами комісії з перевірки та керівником надавача або центрального засвідчувального органу чи уповноваженим ним представником.

5. Член комісії з перевірки, який не погоджується з висновками комісії з перевірки, зазначеними в акті перевірки, зобов'язаний підписати його та письмово викласти свою окрему думку, що долучається до акта перевірки. При цьому перед підписом акта перевірки робиться запис «З окремою думкою, що додається».

6. Якщо керівник надавача або центрального засвідчувального органу чи уповноважений ним представник має зауваження щодо фактів та висновків, викладених в акті перевірки, то перед підписом робить запис «Із зауваженнями, що додаються».

Зауваження до акта перевірки оформлюються окремим документом та підписуються керівником надавача або центрального засвідчувального органу чи уповноваженим ним представником.

Зауваження керівника надавача або центрального засвідчувального органу чи уповноваженого ним представника та окрема думка члена комісії з перевірки є невід'ємною частиною акта перевірки.

7. Якщо керівник надавача або центрального засвідчувального органу чи уповноважений ним представник відмовився від ознайомлення з актом перевірки або від його підписання після ознайомлення з ним, голова комісії з перевірки перед місцем для підпису керівника надавача або центрального засвідчувального органу чи уповноваженого ним представника робить відповідну відмітку, яка засвідчується підписами голови та одного з членів комісії з перевірки.

8. Один примірник акта перевірки залишається в контролюючому органі, другий – у строк не більше п'яти робочих днів після завершення перевірки вручається представнику надавача або центрального засвідчувального органу або надсилається рекомендованим листом з підтвердженням поштового відправлення.

9. У разі перевірки надавача копія акта перевірки протягом п'яти робочих днів після завершення перевірки направляється до центрального засвідчувального органу.

2. Розгляд результатів перевірки

10. За результатами проведення перевірки надавача, його відокремлених пунктів реєстрації або центрального засвідчувального органу контролюючий орган на підставі акта перевірки вживає таких заходів реагування:

1) вимагає усунення порушень вимог законодавства у сфері електронних довірчих послуг в установлений приписом про усунення порушень строк;

2) приймає рішення про блокування кваліфікованого сертифіката відкритого ключа надавача або самопідписаного сертифіката електронної печатки центрального засвідчувального органу в разі, якщо під час перевірки виявлено факти компрометації особистого ключа;

3) надсилає центральному засвідчувальному органу подання про виключення надавача з Довірчого списку в разі виявлення підстав, передбачених частиною п'ятою статті 33 Закону України «Про електронні довірчі послуги».

11. У разі якщо під час проведення перевірки надавача або центрального засвідчувального органу виявлено порушення вимог законодавства у сфері захисту персональних даних, контролюючий орган інформує про такі порушення органи з питань захисту персональних даних.

12. Припис про усунення порушень складається комісією з перевірки протягом п'яти робочих днів з дня завершення перевірки у двох примірниках: один примірник не пізніше п'яти робочих днів з дня складання акта перевірки надається надавачу або центральному засвідчувальному органу, а другий примірник з підписом керівника надавача або центрального засвідчувального органу чи уповноваженого ним представника щодо погоджених термінів усунення порушень вимог законодавства у сфері електронних довірчих послуг залишається в контролюючому органі.

Форма припису про усунення порушень встановлюється спеціально уповноваженим центральним органом виконавчої влади з питань організації спеціального зв'язку та захисту інформації.

Припис про усунення порушень підписується головою та членами комісії з перевірки, які проводили перевірку.

13. У разі відмови керівника надавача або центрального засвідчувального органу чи уповноваженого ним представника від отримання припису про усунення порушень вимог законодавства він направляється рекомендованим листом, а на копії припису про усунення порушень, який залишається в контролюючому органі, проставляються відповідний вихідний номер і дата направлення.

14. Керівник надавача або центрального засвідчувального органу повинен ужити заходів щодо усунення недоліків та порушень, зазначених у приписі про усунення порушень, протягом визначеного у приписі про усунення порушень строку.

15. Надавач або центральний засвідчувальний орган зобов'язаний у встановлений у приписі про усунення порушень строк письмово подати контролюючому органу інформацію про усунення порушень разом з документами, що це підтверджують.

У разі якщо з об'єктивних причин надавач або центральний засвідчувальний орган у встановлений у приписі строк не має можливості усунути порушення, він повідомляє про це контролюючий орган із зазначенням причини та термінів усунення порушення. У такому випадку після усунення порушення надавач або центральний засвідчувальний орган повідомляє контролюючий орган додатково.

16. Рішення про блокування кваліфікованого сертифіката відкритого ключа надавача або самопідписаного сертифіката електронної печатки центрального засвідчувального органу приймається контролюючим органом та в день його прийняття надсилається центральному засвідчувальному органу.

17. Рішення про блокування кваліфікованого сертифіката відкритого ключа надавача або самопідписаного сертифіката електронної печатки центрального засвідчувального органу повинно містити:

1) найменування контролюючого органу;

2) дату прийняття та індекс (порядковий номер);

3) посадовий та персональний склад комісії з перевірки;

4) найменування (прізвище, ім'я, по батькові) надавача або центрального засвідчувального органу;

5) місцезнаходження надавача або центрального засвідчувального органу;

6) прізвище, ім'я та по батькові керівника надавача або центрального засвідчувального органу;

7) обставини, за яких виявлені порушення (тип, строк перевірки, номер та дата акта перевірки або посилання на інше джерело інформації);

8) обґрунтовані підстави прийняття рішення про блокування кваліфікованого сертифіката відкритого ключа надавача або самопідписаного сертифіката електронної печатки центрального засвідчувального органу;

9) вимогу щодо блокування кваліфікованого сертифіката відкритого ключа надавача або самопідписаного сертифіката електронної печатки центрального засвідчувального органу;

10) підпис голови контролюючого органу або його заступника відповідно до розподілу функціональних обов'язків.

18. Центральний засвідчувальний орган на підставі рішення контролюючого органу зобов'язаний змінити статус кваліфікованого сертифіката відкритого ключа надавача або самопідписаного сертифіката електронної печатки центрального засвідчувального органу на заблокований.

19. Подання про виключення надавача з Довірчого списку готується контролюючим органом та в день його підписання головою контролюючого органу надсилається центральному засвідчувальному органу.

20. Подання про виключення надавача з Довірчого списку повинно містити:

1) найменування контролюючого органу;

2) посадовий та персональний склад комісії з перевірки;

3) найменування (прізвище, ім'я, по батькові) надавача;

4) місцезнаходження надавача;

5) прізвище, ім'я та по батькові керівника надавача;

6) обставини, за яких виявлені порушення (тип, строк перевірки, номер та дата акта перевірки або посилання на інше джерело інформації);

7) обґрунтовані підстави прийняття рішення про виключення надавача з Довірчого списку;

8) вимогу щодо виключення надавача з Довірчого списку;

9) дату підписання;

10) підпис голови контролюючого органу або його заступника відповідно до розподілу функціональних обов'язків.

21. У разі виявлення порушень вимог законодавства у сфері електронних довірчих послуг, встановлених для центрального засвідчувального органу, контролюючий орган пропонує центральному засвідчувальному органу шляхи їх усунення.

ЗАТВЕРДЖЕНО
постановою Кабінету Міністрів України
від 2018 р. №

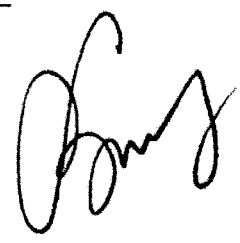
ПЕРЕЛІК
постанов Кабінету Міністрів України, що втратили чинність

1. Постанова Кабінету Міністрів України від 26 травня 2004 року № 680 «Про затвердження Порядку засвідчення наявності електронного документа (електронних даних) на певний момент часу» (Офіційний вісник України, 2004 р., № 21, ст. 1428).

2. Пункт 31 Змін, що вносяться до актів Кабінету Міністрів України, затверджених постановою Кабінету Міністрів України від 08 грудня 2006 року № 1700 (Офіційний вісник України, 2006 р., № 50, ст. 3324).

3. Постанова Кабінету Міністрів України від 27 травня 2013 року № 371 «Про внесення змін до Порядку засвідчення наявності електронного документа (електронних даних) на певний момент часу» (Офіційний вісник України, 2013 р., № 41, ст. 1468).

4. Пункт 2 Змін, що вносяться до постанов Кабінету Міністрів України, затверджених постановою Кабінету Міністрів України від 17 січня 2018 року № 55 (Офіційний вісник України, 2018 р., № 23, ст. 770).



ПОЯСНЮВАЛЬНА ЗАПИСКА

до проекту постанови Кабінету Міністрів України «Про затвердження Вимог у сфері електронних довірчих послуг та Порядку перевірки дотримання вимог законодавства у сфері електронних довірчих послуг»

Мета: підвищення рівня довіри фізичних та юридичних осіб до кваліфікованих електронних довірчих послуг внаслідок врегулювання умов їх надання, а також механізму проведення контролюючим органом заходів державного нагляду (контролю) за дотриманням кваліфікованими надавачами електронних довірчих послуг, їх відокремленими пунктами реєстрації та центральним засвідчувальним органом вимог законодавства у сфері електронних довірчих послуг під час надання кваліфікованих електронних довірчих послуг їх користувачам.

1. Підстава розроблення проекту акта

Проект постанови Кабінету Міністрів України «Про затвердження Вимог у сфері електронних довірчих послуг та Порядку перевірки дотримання вимог законодавства у сфері електронних довірчих послуг» (далі – проект постанови) розроблено на виконання:

статей 13, 18, 19, 20, 21, 23, 26, 27, 28, 33, абзацу третього пункту 8 розділу VII «Прикінцеві та перехідні положення» Закону України «Про електронні довірчі послуги»;

пункти 1910, 1911 плану заходів з виконання Угоди про асоціацію між Україною, з однієї сторони, та Європейським Союзом, Європейським співтовариством з атомної енергії і їхніми державами-членами, з іншої сторони, затвердженого постановою Кабінету Міністрів України від 25 жовтня 2017 року № 1106;

пункту 32 плану пріоритетних дій Уряду на 2018 рік, затвердженого розпорядженням Кабінету Міністрів України від 28 березня 2018 року № 244.

2. Обґрунтування необхідності прийняття акта

Необхідність прийняття проекту постанови полягає у потребі створення умов для надання кваліфікованих електронних довірчих послуг, гармонізованих із положеннями актів законодавства Європейського Союзу, а саме:

Регламенту (ЄС) № 910/2014 Європейського Парламенту та Ради від 23 липня 2014 року щодо електронної ідентифікації та довірчих послуг для цілей електронних транзакцій на внутрішньому ринку, що скасовує Директиву 1999/93/ЄС Європейського Парламенту та Ради;

Імплементаційного рішення Комісії (ЄС) № 2016/650 від 25 квітня 2016 року щодо стандартів оцінки безпеки засобів для створення

кваліфікованих підпису та печатки відповідно до статей 30 (3) та 39 (2) Регламенту (ЄС) № 910/2014 Європейського Парламенту та Ради від 23 липня 2014 року щодо електронної ідентифікації та довірчих послуг для цілей електронних транзакцій на внутрішньому ринку.

Прийняття проекту постанови відповідає зобов'язанням України у зв'язку з ратифікацією Угоди про асоціацію між Україною, з однієї сторони, та Європейським Союзом, Європейським співтовариством з атомної енергії і їхніми державами-членами, з іншої сторони, зокрема пов'язаним із вжиттям заходів, спрямованих на:

забезпечення відповідності вимог до надання електронних довірчих послуг європейським та міжнародним стандартам;

дерегуляцію і розвиток підприємництва та конкуренції;

розвиток галузей електронної торгівлі, науки, технологій та інновацій.

3. Суть проекту акта

Проектом постанови пропонується визначити:

1) організаційно-методологічні, технічні та технологічні умови, яких повинні дотримуватись кваліфіковані надавачі електронних довірчих послуг, їх відокремлені пункти реєстрації та центральний засвідчувальний орган під час надання кваліфікованих електронних довірчих послуг їх користувачам, а саме вимоги до:

кваліфікованих надавачів електронних довірчих послуг;

надання кваліфікованої електронної довірчої послуги створення, перевірки та підтвердження кваліфікованого електронного підпису чи печатки;

надання кваліфікованої електронної довірчої послуги формування, перевірки та підтвердження чинності кваліфікованого сертифіката електронного підпису чи печатки;

надання кваліфікованої електронної довірчої послуги формування, перевірки та підтвердження чинності кваліфікованого сертифіката автентифікації веб-сайту;

надання кваліфікованої електронної довірчої послуги надання кваліфікованої електронної позначки часу;

надання кваліфікованої електронної довірчої послуги реєстрованої електронної доставки;

надання кваліфікованої електронної довірчої послуги зберігання кваліфікованих електронних підписів, печаток, електронних позначок часу та сертифікатів, пов'язаних з такими послугами;

засобів кваліфікованого електронного підпису чи печатки;

кваліфікованих сертифікатів відкритих ключів;

2) перелік стандартів, що застосовуються кваліфікованими надавачами електронних довірчих послуг під час надання кваліфікованих електронних довірчих послуг;

3) механізм проведення контролюючим органом заходів державного нагляду (контролю) за дотриманням вимог законодавства у сфері електронних довірчих послуг, у тому числі, обов'язкових умов, яких повинні дотримуватись кваліфіковані надавачі електронних довірчих послуг, їх відокремлені пункти реєстрації та центральний засвідчувальний орган під час надання кваліфікованих електронних довірчих послуг.

Єдиним способом врегулювання зазначених питань є затвердження проектом постанови:

вимог у сфері електронних довірчих послуг;

порядку перевірки дотримання вимог законодавства у сфері електронних довірчих послуг;

переліку постанов Кабінету Міністрів України, що втратили чинність.

4. Правові аспекти

Правовими підставами розроблення проекту постанови є:

Закон України «Про електронні довірчі послуги»;

план заходів з виконання Угоди про асоціацію між Україною, з однієї сторони, та Європейським Союзом, Європейським співтовариством з атомної енергії і їхніми державами-членами, з іншої сторони, затверджений постановою Кабінету Міністрів України від 25 жовтня 2017 року № 1106;

план пріоритетних дій Уряду на 2018 рік, затверджений розпорядженням Кабінету Міністрів України від 28 березня 2018 року № 244.

У цій сфері правового регулювання діють Закони України «Про електронні довірчі послуги», «Про електронні документи та електронний документообіг», «Про основні засади державного нагляду (контролю) у сфері господарської діяльності», «Про захист інформації в інформаційно-телекомунікаційних системах».

5. Фінансово-економічне обґрунтування

Виходячи з проведеної фінансово-економічної оцінки, реалізація проекту постанови потребуватиме додаткових фінансових витрат з державного бюджету у зв'язку зі зміною організаційно-штатних структур та посиленням заходів захисту інформаційно-телекомунікаційних систем акредитованих центрів сертифікації ключів та центрального засвідчувального органу.

На сьогодні в Україні функціонують 24 акредитовані центри сертифікації ключів, з яких 6 фінансуються за рахунок державного бюджету.

Відповідно до пункту 4 розділу VII «Прикінцеві та перехідні положення» Закону України «Про електронні довірчі послуги» акредитовані центри сертифікації ключів, утворені відповідно до Закону України «Про електронний цифровий підпис», які мають намір надавати кваліфіковані електронні довірчі послуги, автоматично вносяться центральним засвідчувальним органом до Довірчого списку як кваліфіковані надавачі електронних довірчих послуг.

З огляду на зазначене реалізація проекту постанови потребуватиме додаткових фінансових витрат з державного бюджету для 6 акредитованих центрів сертифікації ключів, які фінансуються за рахунок державного бюджету та мають намір надавати кваліфіковані електронні довірчі послуги, а також центрального засвідчувального органу.

Вартість вжиття заходів спрямованих на реалізацію проекту постанови у 2019 році становитиме 6 987,52 тис. грн.

Зведені фінансово-економічні розрахунки до проекту постанови додаються.

6. Прогноз впливу

Реалізація проекту постанови справлятиме вплив на ринкове середовище, забезпечення прав та інтересів суб'єктів господарювання, що мають намір надавати кваліфіковані електронні довірчі послуги.

З огляду на зазначене відповідно до статті 8 Закону України «Про засади державної регуляторної політики у сфері господарської діяльності» підготовлено аналіз регуляторного впливу до проекту постанови.

Реалізація проекту постанови матиме позитивний вплив на ринок праці, а саме збереження існуючих і створення нових робочих місць, підвищення кваліфікації робочої сили та рівня зайнятості населення.

За предметом правового регулювання проект постанови не матиме впливу на:

розвиток регіонів;

громадське здоров'я;

екологію та навколишнє природне середовище.

7. Позиція заінтересованих сторін

Проект постанови підлягає проведенню консультацій з суб'єктами господарювання, що потенційно мають намір надавати кваліфіковані електронні довірчі послуги.

Прогноз впливу реалізації акта на ключові інтереси заінтересованих сторін додається.

За предметом правового регулювання проект постанови не стосується:

питань функціонування місцевого самоврядування, прав та інтересів територіальних громад, місцевого та регіонального розвитку;

соціально-трудової сфери;

прав осіб з інвалідністю;

сфери наукової та науково-технічної діяльності.

8. Громадське обговорення

З метою проведення громадського обговорення проект постанови розміщено на офіційному веб-сайті Міністерства юстиції України та центрального засвідчувального органу.

9. Позиція заінтересованих органів

Проект постанови підлягає погодженню з Міністерством економічного розвитку і торгівлі України, Міністерством фінансів України, Державною службою спеціального зв'язку та захисту інформації України, Державною регуляторною службою України.

10. Правова експертиза

Проект постанови відповідає Конституції України, актам законодавства, що мають вищу юридичну силу, та узгоджується з актами такої ж юридичної сили, не потребує проведення експертизи на відповідність чинним міжнародним договорам України, відповідає вимогам нормопроектувальної техніки, а також Конвенції про захист прав людини і основоположних свобод та практиці Європейського суду з прав людини, крім того, проект постанови не потребує проведення гендерно-правової експертизи.

11. Запобігання дискримінації

У проекті постанови відсутні положення, які містять ознаки дискримінації.

За своєю суттю проект постанови не має впливу на забезпечення рівних прав та можливостей жінок і чоловіків.

Проект постанови не потребує проведення громадської антидискримінаційної експертизи.

12. Запобігання корупції

У проекті постанови відсутні правила і процедури, які можуть містити ризики вчинення корупційних правопорушень.

Проект постанови не потребує проведення громадської антикорупційної експертизи.

13. Прогноз результатів

Прийняття проекту постанови дозволить:

підвищити рівень довіри фізичних та юридичних осіб до кваліфікованих електронних довірчих послуг;

створити сприятливі та конкурентні умови для розвитку та функціонування сфери електронних довірчих послуг;

забезпечити відповідність вимог до надання електронних довірчих послуг європейським та міжнародним стандартам;

забезпечити здійснення контролю за прозорістю та відкритістю у сфері електронних довірчих послуг;

гарантувати доступність та можливість використання кваліфікованих електронних довірчих послуг для людей з обмеженими фізичними можливостями;

забезпечити захист персональних даних, що обробляються під час надання електронних довірчих послуг.

Перший заступник
Міністра юстиції України **Наталія БЕРНАЦЬКА**

«16» серпня 2018 року

ПРОГНОЗ ВПЛИВУ

реалізації проекту постанови Кабінету Міністрів України «Про затвердження Вимог у сфері електронних довірчих послуг та Порядку перевірки дотримання вимог законодавства у сфері електронних довірчих послуг» на ключові інтереси заінтересованих сторін

1. Суть проекту акта

Проект постанови Кабінету Міністрів України «Про затвердження Вимог у сфері електронних довірчих послуг та Порядку перевірки дотримання вимог законодавства у сфері електронних довірчих послуг» спрямований на підвищення рівня довіри фізичних та юридичних осіб до кваліфікованих електронних довірчих послуг внаслідок визначення організаційно-методологічних, технічних та технологічних умов, яких повинні дотримуватись кваліфіковані надавачі електронних довірчих послуг, їх відокремлені пункти реєстрації та центральний засвідчувальний орган під час надання кваліфікованих електронних довірчих послуг їх користувачам.

2. Вплив проекту акта на ключові інтереси заінтересованих сторін

Заінтересована сторона	**Ключовий інтерес**	**Очікуваний (позитивний чи негативний) вплив на ключовий інтерес із зазначенням передбачуваної динаміки змін основних показників (у числовому або якісному вимірі)**		**Пояснення (чому саме реалізація акта призведе до очікуваного впливу)**
		короткостроковий вплив (до року)	**середньостроковий вплив (більше року)**	
Кваліфіковані надавачі електронних довірчих послуг	Приведення діяльності кваліфікованого надавача електронних довірчих послуг у відповідність до нових організаційно-методологічних, технічних та технологічних умов діяльності	**Очікуваний позитивний вплив:** збільшення кількості користувачів кваліфікованих електронних довірчих послуг. **Очікуваний негативний вплив:** збільшення витрат кваліфікованого надавача електронних довірчих послуг	**Очікуваний позитивний вплив:** збільшення прибутку кваліфікованого надавача електронних довірчих послуг	Реалізація акта призведе до збільшення кількості користувачів кваліфікованих електронних довірчих послуг внаслідок розширення спектру кваліфікованих електронних довірчих послуг та покращення якості їх надання кваліфікованими надавачами електронних довірчих послуг. Реалізація акта призведе до збільшення витрат кваліфікованих надавачів електронних довірчих послуг внаслідок запровадження нових організаційно-методологічних, технічних та технологічних умов діяльності у зв'язку з необхідністю зміни організаційно-штатної структури та посиленням заходів захисту інформаційно-телекомунікаційних систем кваліфікованих надавачів електронних довірчих послуг.

				На наступному етапі реалізація акта призведе до збільшення прибутку кваліфікованих надавачів електронних довірчих послуг внаслідок розширення спектру кваліфікованих електронних довірчих послуг та збільшення кількості їх користувачів
Користувачі електронних довірчих послуг	Розширення спектру кваліфікованих електронних довірчих послуг та покращення якості їх надання кваліфікованими надавачами електронних довірчих послуг	**Очікуваний позитивний вплив:** збільшення кількості отриманих кваліфікованих електронних довірчих послуг. **Очікуваний негативний вплив:** збільшення вартості кваліфікованих електронних довірчих послуг	**Очікуваний позитивний вплив:** зменшення витрат на комунікації з органами державної влади, органами місцевого самоврядування, іншими фізичними та юридичними особами	Реалізація акта призведе до збільшення кількості отриманих користувачами кваліфікованих електронних довірчих послуг внаслідок покращення якості надання кваліфікованих електронних довірчих послуг їх надавачами. Реалізація акта призведе до збільшення вартості кваліфікованих електронних довірчих послуг внаслідок збільшення витрат кваліфікованих надавачів електронних довірчих послуг внаслідок запровадження нових організаційно-методологічних, технічних та технологічних умов діяльності з метою розширення спектру кваліфікованих електронних довірчих послуг та покращення якості їх надання. На наступному етапі реалізація акта призведе до зменшення витрат на комунікації з органами державної влади, органами місцевого самоврядування, іншими фізичними та юридичними особами внаслідок підвищення рівня довіри фізичних та юридичних осіб до кваліфікованих електронних довірчих послуг, а також популяризації електронного документообігу та використання засобів електронної ідентифікації

Директор Департаменту приватного права
Міністерства юстиції України **Олена ФЕРЕНС**

ЗВЕДЕНІ ФІНАНСОВО-ЕКОНОМІЧНІ РОЗРАХУНКИ
до проекту постанови Кабінету Міністрів України «Про затвердження Вимог у сфері електронних довірчих послуг та Порядку перевірки дотримання вимог законодавства у сфері електронних довірчих послуг»

Рівень бюджету
Державний бюджет України

Початок реалізації проекту, період, необхідний для його реалізації

Початком реалізації проекту постанови Кабінету Міністрів України «Про затвердження Вимог у сфері електронних довірчих послуг та Порядку перевірки дотримання вимог законодавства у сфері електронних довірчих послуг» (далі – проект постанови) є дата набрання ним чинності.

Проект постанови набирає чинності з дня наступного за днем його опублікування, але не раніше дня набрання чинності Законом України «Про електронні довірчі послуги».

Водночас Закон України «Про електронні довірчі послуги» набирає чинності через рік з дня його опублікування (07 листопада 2018 року), крім статті 10, яка набрала чинності з дня опублікування цього Закону (07 листопада 2017 року).

Строк дії проекту постанови не обмежений у часі.

Аналіз проблеми

Необхідність прийняття проекту постанови полягає у потребі вирішення таких основних проблем:
розширення спектру кваліфікованих електронних довірчих послуг;
підвищення рівня надійності та захищеності електронного документообігу та електронної ідентифікації;
покращення якості надання кваліфікованих електронних довірчих послуг;
підвищення рівня довіри до кваліфікованих електронних довірчих послуг;
популяризація електронного документообігу та використання засобів електронної ідентифікації;
зменшення витрат на комунікації з між фізичними та юридичними особами з державними органам.

Проект постанови спрямований на створення умов для надання кваліфікованих електронних довірчих послуг, гармонізованих із положеннями актів законодавства Європейського Союзу, а саме:

Регламенту (ЄС) № 910/2014 Європейського Парламенту та Ради від 23 липня 2014 року щодо електронної ідентифікації та довірчих послуг для цілей електронних транзакцій на внутрішньому ринку, що скасовує Директиву 1999/93/ЄС Європейського Парламенту та Ради;

Імплементаційного рішення Комісії (ЄС) № 2016/650 від 25 квітня 2016 року щодо стандартів оцінки безпеки засобів для створення кваліфікованих підпису та печатки відповідно до статей 30 (3) та 39 (2) Регламенту (ЄС) № 910/2014 Європейського Парламенту та Ради від 23 липня 2014 року щодо електронної ідентифікації та довірчих послуг для цілей електронних транзакцій на внутрішньому ринку.

Прийняття проекту постанови відповідає зобов'язанням України у зв'язку з ратифікацією Угоди про асоціацію між Україною, з однієї сторони, та Європейським Союзом, Європейським співтовариством з атомної енергії і їхніми державами-членами, з іншої сторони, зокрема пов'язаним із вжиттям заходів, спрямованих на:

забезпечення відповідності вимог до надання електронних довірчих послуг європейським та міжнародним стандартам;

дерегуляцію і розвиток підприємництва та конкуренції;

розвиток галузей електронної торгівлі, науки, технологій та інновацій.

Шляхи реалізації проекту акта та очікувані результати реалізації проекту

Прийняття проекту постанови передбачає продовження реформи законодавства у сфері електронного цифрового підпису, розпочатої у зв'язку з прийняттям Закону України «Про електронні довірчі послуги», шляхом становлення законодавства у сфері електронних довірчих послуг.

Так, проектом постанови пропонується визначити:

1) організаційно-методологічні, технічні та технологічні умови, яких повинні дотримуватись кваліфіковані надавачі електронних довірчих послуг, їх відокремлені пункти реєстрації під час надання кваліфікованих електронних довірчих послуг їх користувачам;

2) механізм проведення контролюючим органом заходів державного нагляду (контролю) за дотриманням вимог законодавства у сфері електронних довірчих послуг, у тому числі, обов'язкових умов, яких повинні дотримуватись кваліфіковані надавачі електронних довірчих послуг, їх відокремлені пункти реєстрації під час надання кваліфікованих електронних довірчих послуг.

Суб'єктами на яких поширюватиметься регулювання проекту постанови є зокрема центри сертифікації ключів, акредитовані центральним засвідчувальним органом в установленому законодавством порядку, та центральний засвідчувальний орган.

Разом з тим відповідно до пункту 4 розділу VII «Прикінцеві та перехідні положення» Закону України «Про електронні довірчі послуги» акредитовані центри сертифікації ключів, утворені відповідно до Закону України «Про електронний цифровий підпис», які мають намір надавати кваліфіковані електронні довірчі послуги, автоматично вносяться центральним засвідчувальним органом до Довірчого списку як кваліфіковані надавачі електронних довірчих послуг протягом року з дня набрання чинності цим Законом.

Станом на сьогодні в Україні функціонують 24 акредитовані центри сертифікації ключів, серед яких 6 фінансуються за рахунок коштів державного бюджету.

Крім того, відповідно до частин четвертої, п'ятої статті 29 Закону України «Про електронні довірчі послуги» центральний засвідчувальний орган під час надання кваліфікованої електронної довірчої послуги формування, перевірки та підтвердження чинності кваліфікованого сертифіката електронного підпису чи печатки зобов'язаний виконувати вимоги, які встановлено для кваліфікованих надавачів електронних довірчих послуг. Програмно-технічний комплекс центрального засвідчувального органу, що використовується ним для надання кваліфікованої електронної довірчої послуги формування, перевірки та підтвердження чинності кваліфікованого сертифіката електронного підпису чи печатки, повинен відповідати вимогам, встановленим для програмно-технічного комплексу кваліфікованих надавачів електронних довірчих послуг.

Реалізація проекту постанови потребуватиме фінансування з державного бюджету для 6 кваліфікованих надавачів електронних довірчих послуг на витрати, пов'язані з:

придбанням основних фондів, обладнання та приладів, сервісне обслуговування, навчання/підвищення кваліфікації персоналу – 130,7 тис. грн для одного кваліфікованого надавача електронних довірчих послуг;

наймом додаткового персоналу (запровадження посади адміністратора аудиту) – 367,22 тис. грн на рік для одного кваліфікованого надавача електронних довірчих послуг.

З огляду на зазначене витрати з державного бюджету для 1 кваліфікованого надавача електронних довірчих послуг складатимуть 497,92 тис. грн, що становитиме 2987,52 тис. грн для 6 кваліфікованих надавачів електронних довірчих послуг.

Крім того, реалізація проекту постанови потребуватиме фінансування з державного бюджету для центрального засвідчувального органу на витрати, пов'язані з:

побудовою програмно-технічного комплексу автоматизації процесів та процедур виконання повноважень центральним засвідчувальним органом – 3 000,00 тис. грн;

наймом додаткового персоналу центрального засвідчувального органу (запровадження посади адміністратора аудиту) – 1 000,00 тис. грн на рік.

З огляду на зазначене витрати з державного бюджету для центрального засвідчувального органу складатимуть 4 000,00 тис. грн.

Розрахунок витрат здійснено на основі інформації, отриманої за результатами консультацій з акредитованими центрами сертифікації ключів та адміністратором інформаційно-телекомунікаційної системи центрального засвідчувального органу.

Зведені фінансово-економічні розрахунки

(тис. грн)

Показники	2019 рік			2020 рік		
	загальний фонд	спеціальний фонд	усього	загальний фонд	спеціальний фонд	усього
1. Витрати бюджету згідно з проектом акта, усього (підпункт 1.1 + підпункт 1.2)	**6 987,52**	**0,00**	**6 987,52**	**3 203,32**	**0,00**	**3 203,32**
1.1. Збільшення витрат (+), усього	**6 987,52**	**0,00**	**6 987,52**	**3 203,32**	**0,00**	**3 203,32**
в межах видатків, передбачених у державному бюджеті на утримання відповідного органу державної влади, органу місцевого самоврядування, підприємства, установи, організації державної форми власності, у тому числі за напрямами використання:						
придбання основних фондів, обладнання та приладів, сервісне обслуговування, навчання/підвищення кваліфікації персоналу для 6 кваліфікованих надавачів електронних довірчих послуг;	784,20	0,00	784,20	0,00	0,00	0,00

найм додаткового персоналу (запровадження посади адміністратора аудиту) для 6 кваліфікованих надавачів електронних довірчих послуг;	2 203,32	0,00	2 203,32	2 203,32	0,00	2 203,32
побудова програмно-технічного комплексу автоматизації процесів та процедур виконання повноважень центральним засвідчувальним органом;	3 000,00	0,00	3 000,00	0,00	0,00	0,00
найм додаткового персоналу центрального засвідчувального органу (запровадження посади адміністратора аудиту)	1 000,00	0,00	1 000,00	1 000,00	0,00	1 000,00
.....						
1.2. Зменшення витрат (–), усього	**0,0**	**0,0**	**0,0**	**0,0**	**0,0**	**0,0**
.....						
2. Надходження до бюджету згідно з проектом акта, усього (підпункт 2.1 + підпункт 2.2)	**0,0**	**0,0**	**0,0**	**0,0**	**0,0**	**0,0**
2.1. Збільшення надходжень (+), усього	**0,0**	**0,0**	**0,0**	**0,0**	**0,0**	**0,0**
.....						
2.2. Зменшення надходжень (–), усього	**0,0**	**0,0**	**0,0**	**0,0**	**0,0**	**0,0**
.....						
3. Витрати бюджету згідно з проектом акта, які враховані у бюджеті, усього	**0,0**	**0,0**	**0,0**	**0,0**	**0,0**	**0,0**
.....						
4. Надходження бюджету згідно з проектом акта, які враховані у бюджеті, – усього	**0,0**	**0,0**	**0,0**	**0,0**	**0,0**	**0,0**
.....						
5. Загальна сума додаткових бюджетних коштів, необхідна згідно з проектом акта (пункт 1 – пункт 2 – пункт 3 – пункт 4)	**6 987,52**	**0,0**	**6 987,52**	**3 203,32**	**0,0**	**3 203,32**
6. Джерела покриття загальної суми додаткових бюджетних коштів (пункт 5), необхідних згідно з проектом акта, усього (підпункт 6.1 + підпункт 6.2)	**0,0**	**0,0**	**0,0**	**0,0**	**0,0**	**0,0**

6.1. Зменшення витрат бюджету (–)всього	**0,0**	**0,0**	**0,0**	**0,0**	**0,0**	**0,0**
6.2. Збільшення доходів бюджету (+) – всього	**0,0**	**0,0**	**0,0**	**0,0**	**0,0**	**0,0**
……						

Директор Департаменту приватного права
Міністерства юстиції України **Олена ФЕРЕНС**

АНАЛІЗ РЕГУЛЯТОРНОГО ВПЛИВУ
проекту постанови Кабінету Міністрів України «Про затвердження Вимог у сфері електронних довірчих послуг та Порядку перевірки дотримання вимог законодавства у сфері електронних довірчих послуг»

І. Визначення проблеми

Проект постанови Кабінету Міністрів України «Про затвердження Вимог у сфері електронних довірчих послуг та Порядку перевірки дотримання вимог законодавства у сфері електронних довірчих послуг» (далі – проект постанови) розроблено на виконання статей 13, 18, 19, 20, 21, 23, 26, 27, 28, 33, абзацу третього пункту 8 розділу VII «Прикінцеві та перехідні положення» Закону України «Про електронні довірчі послуги».

Зазначений Закон набирає чинності через рік з дня його опублікування (07 листопада 2018 року), крім статті 10, яка набрала чинності з дня опублікування цього Закону (07 листопада 2017 року).

Одночасно з набранням чинності Законом України «Про електронні довірчі послуги» втрачає чинність Закон України «Про електронний цифровий підпис».

Суб'єктами на яких поширюватиметься регулювання проекту постанови є зокрема центри сертифікації ключів, акредитовані центральним засвідчувальним органом в установленому порядку відповідно до вимог Закону України «Про електронний цифровий підпис».

Разом з тим відповідно до пункту 4 розділу VII «Прикінцеві та перехідні положення» Закону України «Про електронні довірчі послуги» акредитовані центри сертифікації ключів, утворені відповідно до Закону України «Про електронний цифровий підпис», які мають намір надавати кваліфіковані електронні довірчі послуги, автоматично вносяться центральним засвідчувальним органом до Довірчого списку як кваліфіковані надавачі електронних довірчих послуг протягом року з дня набрання чинності цим Законом.

Станом на сьогодні в Україні функціонують 24 акредитовані центри сертифікації ключів, серед яких 6 не є суб'єктами господарювання.

Крім того, акредитований центр сертифікації ключів приватного акціонерного товариства «Науково-дослідний інститут прикладних інформаційних технологій» повідомив про припинення своєї діяльності з 10 травня 2018 року.

З огляду на зазначене проект постанови поширюватиметься на 17 суб'єктів господарювання.

Необхідність прийняття проекту постанови полягає у потребі вирішення таких основних проблем:

розширення спектру кваліфікованих електронних довірчих послуг;

підвищення рівня надійності та захищеності електронного документообігу та електронної ідентифікації;

покращення якості надання кваліфікованих електронних довірчих послуг;

підвищення рівня довіри до кваліфікованих електронних довірчих послуг;

популяризація електронного документообігу та використання засобів електронної ідентифікації;

зменшення витрат на комунікації з між фізичними та юридичними особами з державними органам.

Проект постанови спрямований на створення умов для надання кваліфікованих електронних довірчих послуг, гармонізованих із положеннями актів законодавства Європейського Союзу, а саме:

Регламенту (ЄС) № 910/2014 Європейського Парламенту та Ради від 23 липня 2014 року щодо електронної ідентифікації та довірчих послуг для цілей електронних транзакцій на внутрішньому ринку, що скасовує Директиву 1999/93/ЄС Європейського Парламенту та Ради;

Імплементаційного рішення Комісії (ЄС) № 2016/650 від 25 квітня 2016 року щодо стандартів оцінки безпеки засобів для створення кваліфікованих підпису та печатки відповідно до статей 30 (3) та 39 (2) Регламенту (ЄС) № 910/2014 Європейського Парламенту та Ради від 23 липня 2014 року щодо електронної ідентифікації та довірчих послуг для цілей електронних транзакцій на внутрішньому ринку.

Прийняття проекту постанови відповідає зобов'язанням України у зв'язку з ратифікацією Угоди про асоціацію між Україною, з однієї сторони, та Європейським Союзом, Європейським співтовариством з атомної енергії і їхніми державами-членами, з іншої сторони, зокрема пов'язаним із вжиттям заходів, спрямованих на:

забезпечення відповідності вимог до надання електронних довірчих послуг європейським та міжнародним стандартам;

дерегуляцію і розвиток підприємництва та конкуренції;

розвиток галузей електронної торгівлі, науки, технологій та інновацій.

Групи (підгрупи)	Так	Ні
Громадяни	Так	
Держава	Так	
Суб'єкти господарювання	Так	

II. Цілі державного регулювання

Проект постанови розроблено з метою підвищення рівня довіри фізичних та юридичних осіб до кваліфікованих електронних довірчих послуг шляхом врегулювання умов їх надання, а також механізму проведення контролюючим органом заходів державного нагляду (контролю) за дотриманням кваліфікованими надавачами електронних довірчих послуг, їх відокремленими пунктами реєстрації вимог законодавства у сфері електронних довірчих послуг під час надання кваліфікованих електронних довірчих послуг їх користувачам.

III. Визначення та оцінка альтернативних способів досягнення цілей

1. Визначення альтернативних способів

Під час розробки проекту постанови було розглянуто такі альтернативні способи досягнення визначених цілей державного регулювання:

Вид альтернативи	Опис альтернативи
Альтернатива 1 Прийняття проекту постанови	Прийняття проекту постанови передбачає продовження реформи законодавства у сфері електронного цифрового підпису, розпочатої у зв'язку з прийняттям Закону України «Про електронні довірчі послуги», шляхом становлення законодавства у сфері електронних довірчих послуг. Так, проектом постанови пропонується визначити: 1) організаційно-методологічні, технічні та технологічні умови, яких повинні дотримуватись кваліфіковані надавачі електронних довірчих послуг, їх відокремлені пункти реєстрації під час надання кваліфікованих електронних довірчих послуг їх користувачам, а саме вимоги до: кваліфікованих надавачів електронних довірчих послуг; надання кваліфікованої електронної довірчої послуги створення, перевірки та підтвердження кваліфікованого електронного підпису чи печатки; надання кваліфікованої електронної довірчої послуги формування, перевірки та підтвердження чинності кваліфікованого сертифіката електронного підпису чи печатки; надання кваліфікованої електронної довірчої послуги формування, перевірки та підтвердження чинності кваліфікованого сертифіката автентифікації веб-сайту; надання кваліфікованої електронної довірчої послуги надання кваліфікованої електронної позначки часу; надання кваліфікованої електронної довірчої послуги реєстрованої електронної доставки; надання кваліфікованої електронної довірчої послуги зберігання кваліфікованих електронних підписів, печаток, електронних позначок часу та сертифікатів, пов'язаних з такими послугами; засобів кваліфікованого електронного підпису чи печатки; кваліфікованих сертифікатів відкритих ключів; 2) перелік стандартів, що застосовуються кваліфікованими надавачами електронних довірчих послуг під час надання кваліфікованих електронних довірчих послуг; 3) механізм проведення контролюючим органом заходів державного нагляду (контролю) за дотриманням вимог законодавства у сфері електронних довірчих послуг, у тому числі, обов'язкових умов, яких повинні дотримуватись кваліфіковані надавачі електронних довірчих послуг, їх відокремлені пункти реєстрації під час надання кваліфікованих електронних довірчих послуг; 4) перелік постанов Кабінету Міністрів України, що втратили чинність
Альтернатива 2 Відсутність регулювання	Відсутність регулювання передбачає залишення існуючого стану справ та зупинення реформи законодавства у сфері електронного цифрового підпису, зокрема ігнорування заходів щодо: 1) виконання зобов'язань України, пов'язаних з ратифікацією

	Угоди про асоціацію між Україною, з однієї сторони, та Європейським Союзом, Європейським співтовариством з атомної енергії і їхніми державами-членами, з іншої сторони, спрямованих на: забезпечення відповідності вимог до надання електронних довірчих послуг європейським та міжнародним стандартам; дерегуляцію і розвиток підприємництва та конкуренції; розвиток галузей електронної торгівлі, науки, технологій та інновацій. 2) гармонізації українського законодавства із законодавством Європейського Союзу, а саме з положеннями Регламенту (ЄС) № 910/2014 Європейського Парламенту та Ради від 23 липня 2014 року щодо електронної ідентифікації та довірчих послуг для цілей електронних транзакцій на внутрішньому ринку, що скасовує Директиву 1999/93/ЄС Європейського Парламенту та Ради, та імплементаційних рішень Європейського Союзу, виданих на виконання зазначеного Регламенту; 3) виконання статей 13, 18, 19, 20, 21, 23, 26, 27, 28, 33, абзацу третього пункту 8 розділу VII «Прикінцеві та перехідні положення» Закону України «Про електронні довірчі послуги»; 4) виконання плану пріоритетних дій Уряду на 2018 рік, затверджений розпорядженням Кабінету Міністрів України від 28 березня 2018 року № 244. Крім того, зазначений альтернативний спосіб державного регулювання призведе до збільшення вразливості кваліфікованих надавачів електронних довірчих послуг як об'єкта критичної інформаційної інфраструктури до кіберзагроз, можливості помилок на добросовісних дій найманих працівників, зменшення якості надання кваліфікованих електронних довірчих послуг та рівня захисту при обробці персональних даних користувачів, внаслідок чого можливе зменшення рівня довіри до роботи кваліфікованих надавачів електронних довірчих послуг на національному рівні, а особливо на рівні транскордонної взаємодії

2. Оцінка вибраних альтернативних способів досягнення цілей

Оцінка впливу на сферу інтересів держави

Вид альтернативи	Вигоди	Витрати
Альтернатива 1 Прийняття проекту постанови	Прийняття проекту постанови матиме такий вплив на інтереси держави: розширення спектру кваліфікованих електронних довірчих послуг; підвищення рівня надійності та захищеності електронного документообігу та електронної ідентифікації; покращення якості надання кваліфікованих електронних довірчих послуг;	Прийняття проекту постанови: призведе до збільшення видатків з державного бюджету внаслідок запровадження нових організаційно-методологічних, технічних та технологічних умов діяльності кваліфікованих надавачів електронних довірчих послу, що фінансуються з державного бюджету, в тому числі, центрального засвідчувального органу; може призвести до збільшення

	підвищення рівня довіри до кваліфікованих електронних довірчих послуг; популяризацію електронного документообігу та використання засобів електронної ідентифікації; зменшення витрат держави на комунікації з іншими фізичними та юридичними особами	вартості кваліфікованих електронних довірчих послуг для їх користувачів (в тому числі органів державної влади) внаслідок збільшення витрат кваліфікованих надавачів електронних довірчих послуг внаслідок запровадження нових організаційно-методологічних, технічних та технологічних умов діяльності з метою розширення спектру кваліфікованих електронних довірчих послуг та покращення якості їх надання; може призвести до збільшення витрат контролюючого органу, пов'язаних з адмініструванням заходів державного нагляду (контролю). Розрахунок відповідних витрат здійснено у розділі VI
Альтернатива 2 Відсутність регулювання	Відсутність регулювання означає залишення існуючого стану справ, що не передбачає жодних вигод для держави	Відсутність регулювання означає залишення існуючого стану справ, що не матиме такого впливу на інтереси держави: розширення спектру кваліфікованих електронних довірчих послуг; підвищення рівня надійності та захищеності електронного документообігу та електронної ідентифікації; покращення якості надання кваліфікованих електронних довірчих послуг; підвищення рівня довіри до кваліфікованих електронних довірчих послуг; популяризацію електронного документообігу та використання засобів електронної ідентифікації; зменшення витрат держави на комунікації з іншими фізичними та юридичними особами

Оцінка впливу на сферу інтересів громадян

Вид альтернативи	Вигоди	Витрати
Альтернатива 1 Прийняття проекту постанови	Прийняття проекту постанови матиме такий вплив на інтереси громадян: розширення спектру	Прийняття проекту постанови може призвести до збільшення вартості кваліфікованих електронних довірчих послуг для

	кваліфікованих електронних довірчих послуг; підвищення рівня надійності та захищеності електронного документообігу та електронної ідентифікації; покращення якості надання кваліфікованих електронних довірчих послуг; підвищення рівня довіри до кваліфікованих електронних довірчих послуг; популяризацію електронного документообігу та використання засобів електронної ідентифікації; зменшення витрат держави на комунікації з іншими фізичними та юридичними особами	їх користувачів (в тому числі громадян) внаслідок збільшення витрат кваліфікованих надавачів електронних довірчих послуг, пов'язаних із запровадженням нових організаційно-методологічних, технічних та технологічних умов діяльності з метою розширення спектру кваліфікованих електронних довірчих послуг та покращення якості їх надання
Альтернатива 2 Відсутність регулювання	Відсутність регулювання означає залишення існуючого стану справ, що не передбачає жодних вигод для громадян	Відсутність регулювання означає залишення існуючого стану справ, що не матиме такого впливу на інтереси громадян: розширення спектру кваліфікованих електронних довірчих послуг; підвищення рівня надійності та захищеності електронного документообігу та електронної ідентифікації; покращення якості надання кваліфікованих електронних довірчих послуг; підвищення рівня довіри до кваліфікованих електронних довірчих послуг; популяризацію електронного документообігу та використання засобів електронної ідентифікації; зменшення витрат держави на комунікації з іншими фізичними та юридичними особами

Оцінка впливу на сферу інтересів суб'єктів господарювання

Показник	Великі	Середні	Малі	Мікро	Разом
Кількість суб'єктів господарювання, що підпадають під дію регулювання, одиниць	0	17	0	0	17
Питома вага групи у загальній кількості, відсотків	0	100	0	0	100

Вид альтернативи	Вигоди	Витрати
Альтернатива 1 Прийняття проекту постанови	Прийняття проекту постанови матиме такий вплив на інтереси суб'єктів господарювання: розширення спектру кваліфікованих електронних довірчих послуг; покращення якості надання кваліфікованих електронних довірчих послуг; підвищення рівня довіри до кваліфікованих електронних довірчих послуг; збільшення кількості користувачів кваліфікованих електронних довірчих послуг; збільшення прибутку суб'єкта господарювання	Прийняття проекту постанови призведе до збільшення витрат суб'єкта господарювання внаслідок запровадження нових організаційно-методологічних, технічних та технологічних умов діяльності з метою розширення спектру кваліфікованих електронних довірчих послуг та покращення якості їх надання
Альтернатива 2 Відсутність регулювання	Відсутність регулювання означає залишення існуючого стану справ, що не передбачає жодних вигод для суб'єктів господарювання	Відсутність регулювання означає залишення існуючого стану справ, що не матиме такого впливу на інтереси суб'єктів господарювання: розширення спектру кваліфікованих електронних довірчих послуг; покращення якості надання кваліфікованих електронних довірчих послуг; підвищення рівня довіри до кваліфікованих електронних довірчих послуг; збільшення кількості користувачів кваліфікованих електронних довірчих послуг; збільшення прибутку суб'єкта господарювання

ВИТРАТИ
на одного суб'єкта господарювання великого і середнього підприємництва, які виникають внаслідок дії регуляторного акта

Порядковий номер	Витрати	За перший рік	За п'ять років
1.	**Витрати на придбання основних фондів, обладнання та приладів, сервісне обслуговування, навчання / підвищення кваліфікації персоналу тощо, гривень:**	**180 700,00**	**195 700,00**
1.1.	проведення модернізації комплексної системи захисту інформації в інформаційно-телекомунікаційній системі кваліфікованого	130 700,00	130 700,00

	надавача електронних довірчих послуг (придбання обладнання, приладів та ліцензійного програмного забезпечення)		
1.2.	переобладнання спеціальних приміщень кваліфікованого надавача електронних довірчих послуг для можливості доступу осіб з обмеженими фізичними можливостями та інших маломобільних груп населення	20 000,00	20 000,00
1.3.	доопрацювання офіційного веб-сайту кваліфікованого надавача електронних довірчих послуг з метою забезпечення доступності інформації для осіб з обмеженими фізичними можливостями, зокрема для користувачів з вадами зору та слуху	15 000,00	15 000,00
1.4.	підвищення кваліфікації найманих працівників кваліфікованого надавача електронних довірчих послуг (5 осіб х 3 000,00 грн) у сферах інформаційних технологій, захисту інформації або кібербезпеки та захисту персональних даних	15 000,00	30 000,00
2.	**Витрати, пов'язані із веденням обліку, підготовкою та поданням звітності державним органам, гривень**	**200,00**	**1 000,00**
2.1.	підготовка щорічного звіту для контролюючого органу про діяльність кваліфікованого надавача електронних довірчих послуг	200,00	1 000,00
3.	**Витрати, пов'язані з адмініструванням заходів державного нагляду (контролю) (перевірок, штрафних санкцій, виконання рішень/приписів тощо), гривень**	**2 200,00**	**4 400, 00**
3.1.	Витрати пов'язані з адмініструванням виїзних перевірок	2 200,00	4 400, 00
4.	**Витрати на отримання адміністративних послуг (дозволів, ліцензій, сертифікатів, атестатів, погоджень, висновків, проведення незалежних/обов'язкових експертиз, сертифікації, атестації тощо) та інших послуг (проведення наукових, інших експертиз, страхування тощо), гривень:**	**162 800,00**	**163 000,00**
4.1.	погодження регламенту роботи кваліфікованого надавача електронних довірчих послуг	200,00	400,00
4.2.	проведення додаткової державної експертизи комплексної системи захисту інформації інформаційно-телекомунікаційної системи кваліфікованого надавача електронних довірчих послуг	162 600,00	162 600,00
5.	**Витрати на оборотні активи (матеріали, канцелярські товари тощо), гривень**	**1 000,00**	**5 000,00**
6.	**Витрати, пов'язані із наймом додаткового персоналу, гривень:**	**44 700,00**	**223 500,00**
6.1.	введення посади адміністратора аудиту до складу найманих осіб кваліфікованого надавача електронних довірчих послуг (мінімальна	44 700,00	223 500,00

	заробітна плата у місячному розмірі: з 1 січня 2018 року – 3723,00 гривні)		
7	**РАЗОМ (сума рядків: 1 + 2 + 3 + 4 + 5 + 6), гривень**	**346 900,00**	**592 600,00**

Сумарні витрати за альтернативами	Сума витрат, гривень
Альтернатива 1 Прийняття проекту постанови	346 900,00
Альтернатива 2 Відсутність регулювання	0,00

Оцінка впливу на сферу інтересів суб'єктів господарювання проведена на основі узагальнення інформації, наданої суб'єктами господарювання у сфері електронного цифрового підпису.

IV. Вибір найбільш оптимального альтернативного способу досягнення цілей

За результатами аналізу альтернативних способів досягнення цілей державного регулювання здійснено вибір оптимального альтернативного способу з урахуванням системи бальної оцінки ступеня досягнення визначених цілей.

Бал результативності визначається за чотирибальною системою оцінки ступеня досягнення визначених цілей державного регулювання.

Рейтинг результативності (досягнення цілей під час вирішення проблеми)	Бал результативності (за чотирибальною системою оцінки)	Коментарі щодо присвоєння відповідного бала
Альтернатива 1 Прийняття проекту постанови	4	Прийняття проекту постанови сприятиме: розширенню спектру кваліфікованих електронних довірчих послуг; покращенню якості надання кваліфікованих електронних довірчих послуг; підвищенню рівня довіри до кваліфікованих електронних довірчих послуг; збільшенню кількості користувачів кваліфікованих електронних довірчих послуг; збільшенню прибутку суб'єктів господарювання
Альтернатива 2 Відсутність регулювання	1	Відсутність регулювання передбачає залишення існуючого стану справ та зупинення реформи законодавства у сфері електронного цифрового підпису

Рейтинг результативності	Вигоди (підсумок)	Витрати (підсумок)	Обґрунтування відповідного місця альтернативи у

			рейтингу
Альтернатива 1 Прийняття проекту постанови	Прийняття проекту постанови сприятиме: розширенню спектру кваліфікованих електронних довірчих послуг; підвищення рівня надійності та захищеності електронного документообігу та електронної ідентифікації; покращенню якості надання кваліфікованих електронних довірчих послуг; підвищенню рівня довіри до кваліфікованих електронних довірчих послуг; збільшенню кількості користувачів кваліфікованих електронних довірчих послуг; популяризацію електронного документообігу та використання засобів електронної ідентифікації; зменшення витрат держави на комунікації з іншими фізичними та юридичними особами; збільшенню прибутку суб'єктів господарювання	Прийняття проекту постанови може призвести до збільшення вартості кваліфікованих електронних довірчих послуг для їх користувачів внаслідок збільшення витрат кваліфікованих надавачів електронних довірчих послуг, пов'язаних із запровадженням нових організаційно-методологічних, технічних та технологічних умов діяльності з метою розширення спектру кваліфікованих електронних довірчих послуг та покращення якості їх надання	Цілі, визначені стратегічним документами досягнуті
Альтернатива 2 Відсутність регулювання	Відсутність регулювання означає залишення існуючого стану справ, що не передбачає жодних вигод для держави, громадян та суб'єктів господарювання	Відсутність регулювання означає залишення існуючого стану справ, що не передбачає жодних витрат для держави, громадян та суб'єктів господарювання	Недосягнення цілей, визначених стратегічними документами

V. Механізми та заходи, які забезпечать розв'язання визначеної проблеми

Основним механізмами, які забезпечують розв'язання визначеної проблеми, є затвердження:

Вимог у сфері електронних довірчих послуг шляхом визначення організаційно-методологічних, технічних та технологічних умов, яких повинні дотримуватись кваліфіковані надавачі електронних довірчих послуг, їх

відокремлені пункти реєстрації під час надання кваліфікованих електронних довірчих послуг їх користувачам, а також переліку стандартів, що застосовуються кваліфікованими надавачами електронних довірчих послуг під час надання кваліфікованих електронних довірчих послуг;

Порядку перевірки дотримання вимог законодавства у сфері електронних довірчих послуг шляхом визначення механізму проведення контролюючим органом заходів державного нагляду (контролю) за дотриманням вимог законодавства у сфері електронних довірчих послуг, у тому числі, обов'язкових умов, яких повинні дотримуватись кваліфіковані надавачі електронних довірчих послуг, їх відокремлені пункти реєстрації під час надання кваліфікованих електронних довірчих послуг.

Заходами, спрямованими на розв'язання визначеної проблеми є:

розробка проекту постанови;

громадське обговорення проекту постанови;

погодження проекту постанови із заінтересованими органами;

врахування зауважень та пропозицій до проекту постанови, наданих фізичними та юридичними особами, зокрема заінтересованими органами;

подання проекту постанови на розгляд Кабінету Міністрів України;

супровід проекту постанови під час його розгляду в Кабінеті Міністрів України;

прийняття постанови Кабінету Міністрів України «Про затвердження Вимог у сфері електронних довірчих послуг та Порядку перевірки дотримання вимог законодавства у сфері електронних довірчих послуг».

VI. Оцінка виконання вимог регуляторного акта залежно від ресурсів, якими розпоряджаються органи виконавчої влади чи органи місцевого самоврядування, фізичні та юридичні особи, які повинні проваджувати або виконувати ці вимоги

БЮДЖЕТНІ ВИТРАТИ
на адміністрування регулювання для суб'єктів великого і середнього підприємництва

Процедура регулювання суб'єктів великого і середнього підприємництва (розрахунок на одного типового суб'єкта господарювання)	Планові витрати часу на процедуру	Вартість часу співробітника органу державної влади відповідної категорії (заробітна плата)	Оцінка кількості процедур за рік, що припадають на одного суб'єкта	Оцінка кількості суб'єктів, що підпадають під дію процедури регулювання	Витрати на адміністрування регулювання (за рік), гривень
1. Облік суб'єкта господарювання, що перебуває у сфері регулювання	**2 робочі дні**	**400,00 грн за робочий день (з розрахунку 9 000,00 грн за місяць)**	**2**	**24**	**800,00**

Адміністрація Державної служби спеціального зв'язку та захисту інформації України	1 робочий день	400,00 грн за робочий день (з розрахунку 9 000,00 грн за місяць)	1	24	400,00
Міністерство юстиції України	1 робочий день	400,00 грн за робочий день (з розрахунку 9 000,00 грн за місяць)	1	24	400,00
2. Поточний контроль за суб'єктом господарювання, що перебуває у сфері регулювання, у тому числі:	**15 робочих днів**	**400,00 грн за робочий день (з розрахунку 9 000,00 грн за місяць)**	**2**	**24**	**6 000,00**
камеральні (Адміністрація Державної служби спеціального зв'язку та захисту інформації України)	5 робочих днів	400,00 грн за робочий день (з розрахунку 9 000,00 грн за місяць)	1	24	2 000,00
виїзні (Адміністрація Державної служби спеціального зв'язку та захисту інформації України)	10 робочих днів	400,00 грн за робочий день (з розрахунку 9 000,00 грн за місяць)	1	24	4 000,00
3. Підготовка, затвердження та опрацювання одного окремого акта про порушення вимог регулювання (Адміністрація Державної служби спеціального зв'язку та захисту інформації України)	**1 робочий день**	**400,00 грн за робочий день (з розрахунку 9 000,00 грн за місяць)**	**1**	**24**	**400,00**
4. Реалізація одного окремого рішення щодо порушення вимог регулювання	**2 робочі дні**	**400,00 грн за робочий день (з розрахунку 9 000,00 грн за місяць)**	**2**	**24**	**800,00**
Адміністрація	1 робочий	400,00 грн за	1	24	400,00

Державної служби спеціального зв'язку та захисту інформації України	день	робочий день (з розрахунку 9 000,00 грн за місяць)			
Міністерство юстиції України	1 робочий день	400,00 грн за робочий день (з розрахунку 9 000,00 грн за місяць)	1	24	400,00
5. Оскарження одного окремого рішення суб'єктами господарювання	**2 робочі дні**	**400,00 грн за робочий день (з розрахунку 9 000,00 грн за місяць)**	**2**	**24**	**800,00**
Адміністрація Державної служби спеціального зв'язку та захисту інформації України	1 робочий день	400,00 грн за робочий день (з розрахунку 9 000,00 грн за місяць)	1	24	400,00
Міністерство юстиції України	1 робочий день	400,00 грн за робочий день (з розрахунку 9 000,00 грн за місяць)	1	24	400,00
6. Підготовка звітності за результатами регулювання (Адміністрація Державної служби спеціального зв'язку та захисту інформації України)	**2 робочі дні**	**400,00 грн за робочий день (з розрахунку 9 000,00 грн за місяць)**	**1**	**24**	**800,00**
Разом за рік	**24 робочі дні**	**400,00 грн за робочий день (з розрахунку 9 000,00 грн за місяць)**	**10**	**24**	**9 600,00**
Сумарно за п'ять років	**120**	**400,00 грн за робочий день (з розрахунку 9 000,00 грн за місяць)**	**50**	**24**	**48 000,00**

Порядковий номер	Назва державного органу	Витрати на адміністрування регулювання за рік, гривень	Сумарні витрати на адміністрування регулювання за п'ять років, гривень
Сумарно бюджетні витрати на адміністрування регулювання суб'єктів великого і середнього підприємництва	Адміністрація Державної служби спеціального зв'язку та захисту інформації України	8 400,00	42 000,00
	Міністерство юстиції України	1 200,00	6 000,00

VII. Обґрунтування запропонованого строку дії регуляторного акта

Строк дії проекту постанови не обмежений у часі.

Зміна строку дії проекту постанови можлива у разі прийняття змін до нього, прийняття змін до нормативно-правових актів, що мають вищу юридичну силу, які стосуються цієї сфери регулювання, або визнання зазначених актів такими, що втратили чинність

Проект постанови набирає чинності з дня наступного за днем її опублікування, але не раніше дня набрання чинності Законом України «Про електронні довірчі послуги».

VIII. Визначення показників результативності дії регуляторного акта

Показники результативності дії регуляторного акта:

розмір надходжень до державного та місцевих бюджетів і державних цільових фондів, пов'язаних з дією акта, внаслідок прибутку одержаного кваліфікованими надавачами електронних довірчих послуг (оцінюватиметься через рік з дня набрання чинності проектом постанови);

кількість суб'єктів господарювання та/або фізичних осіб, на яких поширюватиметься дія акта (17 суб'єкта господарювання, що відповідно до пункту 4 розділу VII «Прикінцеві та перехідні положення» Закону України «Про електронні довірчі послуги» будуть автоматично внесені центральним засвідчувальним органом до Довірчого списку як кваліфіковані надавачі електронних довірчих послуг);

розмір коштів і час, що витрачатимуться суб'єктами господарювання та/або фізичними особами, пов'язаними з виконанням вимог акта (розрахунок наведено у Витратах на одного суб'єкта господарювання);

рівень поінформованості суб'єктів господарювання та/або фізичних осіб з основних положень акта (високий, – оскільки проект постанови розміщено на офіційних веб-сайтах Міністерства юстиції України та центрального засвідчувального органу, про що Міністерством юстиції України повідомлено 17 суб'єкта господарювання);

кількість користувачів кваліфікованих електронних довірчих послуг (оцінюватиметься через рік з дня набрання чинності проектом постанови);

кількість електронних сервісів органів державної влади, електронна ідентифікація в яких здійснюватиметься на підставі електронних довірчих послуг (оцінюватиметься через рік з дня набрання чинності проектом постанови);

кількість виявлених контролюючим органом порушень законодавства у сфері електронних довірчих послуг (оцінюватиметься через рік з дня набрання чинності проектом постанови).

IX. Визначення заходів, за допомогою яких здійснюватиметься відстеження результативності дії регуляторного акта

Відповідно до законодавства здійснюється базове, повторне та періодичне відстеження результативності регуляторного акта у строки, встановлені статтею 10 Закону України «Про засади державної регуляторної політики у сфері господарської діяльності».

Базове відстеження результативності проекту постанови буде здійснюватись через рік після набрання чинності зазначеною постановою, оскільки планується використовувати статистичний метод відстеження та статистичні дані.

Повторне відстеження планується здійснити через рік після проведення базового відстеження на основі порівняння показників базового та повторного відстеження.

Періодичні відстеження планується здійснювати раз на три роки, починаючи з дня проведення повторного відстеження. Установлені показники результативності акта порівнюватимуться із значеннями аналогічних показників, що встановлені під час повторного відстеження.

Джерело даних: статистичні дані, отримані від центрального засвідчувального органу, контролюючого органу та кваліфікованих надавачів електронних довірчих послуг.

Виконавець заходів з відстеження результативності проекту постанови – Міністерство юстиції України.

Перший заступник
Міністра юстиції України **Наталія БЕРНАЦЬКА**

«16» серпня 2018 року

(/def

(/)

ПОВІДОМЛЕННЯ ПРО ОПРИЛЮДНЕННЯ РЕГУЛЯТОРНИХ АКТІВ, ЩО РОЗРОБЛЕНІ МІНІСТЕРСТВОМ ЮСТИЦІЇ

Проект постанови Кабінету Міністрів України "Про затвердження Вимог у сфері електронних довірчих послуг та Порядку перевірки дотримання вимог законодавства у сфері електронних довірчих послуг" (/files/general/2018/08/17/20180817121312-12.pdf)

ПОЯСНЮВАЛЬНА ЗАПИСКА до проекту постанови Кабінету Міністрів України «Про затвердження Вимог у сфері електронних довірчих послуг та Порядку перевірки дотримання вимог законодавства у сфері електронних довірчих послуг» (/files/general/2018/08/17/20180817115812-46.doc)

АНАЛІЗ РЕГУЛЯТОРНОГО ВПЛИВУ проекту постанови Кабінету Міністрів України «Про затвердження Вимог у сфері електронних довірчих послуг та Порядку перевірки дотримання вимог законодавства у сфері електронних довірчих послуг» (/files/general/2018/08/17/20180817115813-37.doc)

Повідомлення про оприлюднення проекту постанови Кабінету Міністрів України «Про затвердження Вимог у сфері електронних довірчих послуг та Порядку перевірки дотримання вимог законодавства у сфері електронних довірчих послуг» (/files/general/2018/08/17/20180817115813-45.doc)

Проект постанови Кабінету Міністрів України "Про затвердження Порядку зберігання документованої інформації та її передавання центральному засвідчувальному органу в разі припинення діяльності кваліфікованого надавача електронних довірчих послуг" (/files/general/2018/08/10/20180810141743-77.doc)

АКТ про приймання-передавання документованої інформації кваліфікованого надавача електронних довірчих послуг на зберігання до центрального засвідчувального органу (/files/general/2018/08/10/20180810141743-31.doc)

Повідомлення про оприлюднення проекту постанови Кабінету Міністрів України «Про затвердження Вимог у сфері електронних довірчих послуг та Порядку перевірки дотримання вимог законодавства у сфері електронних довірчих послуг»

Відповідно до статті 9 Закону України «Про засади державної регуляторної політики у сфері господарської діяльності» Міністерство юстиції України повідомляє про оприлюднення на офіційному веб-сайті Міністерства юстиції України проекту постанови Кабінету Міністрів України «Про затвердження Вимог у сфері електронних довірчих послуг та Порядку перевірки дотримання вимог законодавства у сфері електронних довірчих послуг» (далі – проект постанови) з метою одержання зауважень і пропозицій від фізичних та юридичних осіб, їх об'єднань.

Проект постанови розроблено на виконання статей 13, 18, 19, 20, 21, 23, 26, 27, 28, 33, абзацу третього пункту 8 розділу VII «Прикінцеві та перехідні положення» Закону України «Про електронні довірчі послуги» з метою підвищення рівня довіри фізичних та юридичних осіб до кваліфікованих електронних довірчих послуг шляхом врегулювання умов їх надання, а також механізму проведення контролюючим органом заходів державного нагляду (контролю) за дотриманням кваліфікованими надавачами електронних довірчих послуг, їх відокремленими пунктами реєстрації вимог законодавства у сфері електронних довірчих послуг під час надання кваліфікованих електронних довірчих послуг їх користувачам.

Зауваження та пропозиції до проекту постанови просимо надсилати протягом одного місяця з дня його оприлюднення за адресою: Міністерство юстиції України, вул. Городецького, 13, м. Київ, 01001, а також за адресою електронної пошти: ecp@minjust.gov.ua.

Директор Департаменту приватного права **Олена ФЕРЕНС**

МІНІСТЕРСТВО ЮСТИЦІЇ УКРАЇНИ

Україна, 01001, м. Київ, вул. Городецького, буд. 13, тел. (044) 271-16-37, 271-16-36

16.08.2018 № 14-7937

ДОВІДКА

Видана про те, що відповідно до наказу Міністерства юстиції України від 15 серпня 2018 року № 937/6 обов'язки Міністра юстиції України 16 серпня 2018 року виконує перший заступник Міністра юстиції **Бернацька Наталія Іларіонівна.**

Заступник директора департаменту – начальник Управління персоналу центрального апарату Департаменту персоналу **О.В.Кушніренко**