

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 (далі – користувачі).

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

1. 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;

дані створення електронного підпису чи печатки – унікальний набір даних, що використовується користувачем при створенні електронного підпису чи печатки;

захищений носій особистого ключа – засіб кваліфікованого електронного підпису чи печатки, що призначений для зберігання особистого ключа та має вбудовані апаратно-програмні засоби, що забезпечують захист записаних на нього даних від несанкціонованого доступу, від безпосереднього ознайомлення із значенням параметрів особистого ключа та їх копіювання;

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

інформаційно-телекомунікаційна система надавача – організаційно-технічна система надавача, центрального засвідчувального органу, що забезпечує обслуговування кваліфікованих сертифікатів відкритих ключів та об'єднує програмно-технічний комплекс, що використовується під час надання кваліфікованих електронних довірчих послуг (далі – програмно-технічний комплекс), фізичне середовище, найманих працівників надавача, а також інформацію, що обробляється в ній;

кваліфікована електронна довірча послуга – електронна довірча послуга, що надається надавачем за допомогою засобу кваліфікованого електронного підпису чи печатки та базується на кваліфікованому сертифікаті відкритого ключа;

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 в процесі надання електронних довірчих послуг з обслуговування кваліфікованих сертифікатів електронного підпису чи печатки, 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 користувачам;

регламент роботи надавача – нормативний документ, що визначає організаційно-методологічні, технічні та технологічні умови діяльності надавача під час надання кваліфікованих електронних довірчих послуг, включаючи політику та порядок сертифікації;

реєстрація користувача – встановлення особи заявника та перевірка його ідентифікаційних даних, що вносяться до його кваліфікованого сертифіката відкритого ключа;

розпізнавальне ім'я – сукупність реквізитів користувача, що забезпечують можливість однозначного визначення належності кваліфікованого сертифіката відкритого ключа цьому користувачу серед інших кваліфікованих сертифікатів відкритих ключів, сформованих надавачем;

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

сертифікація користувача – формування кваліфікованого сертифіката відкритого ключа, на підставі ідентифікаційних даних, перевірених під час реєстрації користувача, та накладання на такий кваліфікований сертифікат відкритого ключа кваліфікованого електронного підпису чи печатки надавача;

спеціальні приміщення – нежилі приміщення, які використовуються надавачем для розміщення всіх складових програмно-технічного комплексу;

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.

2. Інші терміни вживаються у значеннях, наведених в Законах України «Про електронні довірчі послуги», «Про електронні документи та електронний

документообіг», «Про телекомунікації», «Про захист інформації в інформаційно-телекомунікаційних системах».

Розділ II. Вимоги до надавачів

1. Вимоги до найманих працівників надавача

1. Наймані працівники надавача повинні мати необхідні для надання кваліфікованих електронних довірчих послуг знання, досвід і кваліфікацію, у тому числі у сферах інформаційних технологій, захисту інформації або кібербезпеки.

Наймані працівники надавача, обов'язки яких будуть безпосередньо пов'язані з наданням кваліфікованих електронних довірчих послуг, повинні мати трирічний стаж роботи за фахом.

2. Організаційно-правовий статус найманого працівника надавача, його функції та завдання, права та обов'язки, відповідальність в межах організації, а також професійні знання, досвід та кваліфікацію визначає посадова інструкція.

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

3. Керівник надавача повинен гарантувати, що найманий працівник надавача, обов'язки якого будуть безпосередньо пов'язані з наданням кваліфікованих електронних довірчих послуг, ознайомлений з вимогами своєї посадової інструкції та погоджується з ними.

Керівник надавача повинен демонструвати підтримку вимог інформаційної безпеки та методів її забезпечення, а також діяти відповідно до своїх посадових функцій та завдань.

4. 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.

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 користувачу особистого ключа та його відповідності відкритому ключу користувача;
- 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 особистого ключа надавача, а також створення їх резервних копій.

8. Основними обов'язками адміністратора сертифікації є:

- 1) участь у генерації пари ключів надавача та зберігання його особистих ключів та їх резервних копій;
- 2) забезпечення використання особистих ключів надавача під час формування та обслуговування кваліфікованих сертифікатів відкритих ключів надавача та користувачів;
- 3) перевірка заяв про формування кваліфікованих сертифікатів відкритих ключів вимогам регламенту роботи надавача;
- 4) участь у знищенні особистих ключів надавача;
- 5) забезпечення ведення, архівування та відновлення баз даних кваліфікованих сертифікатів відкритих ключів користувачів;
- 6) публікація кваліфікованих сертифікатів відкритих ключів користувачів та списків відкликаних сертифікатів відкритих ключів на офіційному веб-сайті надавача;
- 7) резервування кваліфікованих сертифікатів відкритих ключів надавача, користувачів, списків відкликаних сертифікатів відкритих ключів 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 пари ключів надавача та їх резервних копій;

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

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 (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 після збоїв, відмов, аварій інформаційно-телекомунікаційної системи надавача;

8) забезпечення режиму доступу до спеціальних приміщень інформаційно-телекомунікаційної системи 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 його 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 внутрішніх перевірок діяльності надавача на відповідність нормативно-правовим документам у сферах електронних довірчих послуг та кібербезпеки. Надавач встановлює періодичність (у днях, тижнях або місяцях) проведення таких внутрішніх перевірок, але не рідше, ніж раз на 6 місяців.

14) Обов'язки адміністратора аудиту:

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

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 бази даних надавача;

5) контроль за веденням архіву надавача.

15. Наймані працівники надавача повинні бути повідомлені про зміни в організації процесів надавача, що стосуються його 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 документації на комплексну систему захисту інформації або систему управління інформаційною безпекою.

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

1. 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 шкоди, яка може бути завдана користувачам таких послуг чи третім особам.

2. 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».

3. 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.

3. Управління ризиками

1. Надавач зобов'язаний здійснювати управління ризиками для визначення, аналізу та оцінки можливих ризиків при наданні електронних довірчих послуг з урахуванням економічних та технічних проблем.

2. Надавач обирає відповідні заходи з нейтралізації ризиків з урахуванням результатів визначення, аналізу та оцінки ризиків.

Заходи з нейтралізації ризиків повинні гарантувати, що рівень безпеки відповідає ступеню ризику.

3. Визначені надавачем заходи безпеки та операційні процедури, які необхідні для реалізації обраних ним заходів з управління ризиками, повинні бути зафіксовані в документах на комплексну систему захисту інформації або систему управління інформаційною безпекою та в регламенті роботи надавача.

4. Управління ризиками та заходи з їх нейтралізації повинні регулярно переглядатися.

5. Звіт з управління ризиками, що включає перелік, аналіз та оцінки можливих ризиків, включаючи оцінений залишковий ризик, затверджується керівником надавача.

4. Вимоги до захисту інформації та інформаційних ресурсів надавача

Організаційні питання

1. Безпека інформаційних ресурсів надавача досягається шляхом впровадження організаційних, інженерно-технічних заходів, засобів і методів технічного та криптографічного захисту інформації комплексної системи захисту інформації, спрямованих на забезпечення захисту інформації під час надання електронних довірчих послуг.

2. Відповідність комплексної системи захисту інформації вимогам нормативних документів у сфері захисту інформації підтверджується атестатом відповідності та позитивним експертним висновком за результатами державної експертизи у сфері криптографічного захисту інформації або документом про

відповідність, складеного за результатами проведення процедури оцінки відповідності у сфері електронних довірчих послуг.

3. Надання кваліфікованих електронних довірчих послуг надавачем без чинних документів, визначених законодавством, що підтверджують відповідність комплексної системи захисту інформації інформаційно-телекомунікаційної системи надавача та засобів захисту інформації у її складі вимогам нормативно-правових актів у сфері технічного та криптографічного захисту інформації, або документів про відповідність за результатами проходження процедури оцінки відповідності у сфері електронних довірчих послуг забороняється.

4. Захист інформації надавача забезпечується службою захисту інформації, до складу якої входять:

- 1) посадова особа надавача, на яку наказом керівника надавача покладено обов'язки керівника служби захисту інформації;
- 2) адміністратор безпеки;
- 3) системний адміністратор.

5. Служба захисту інформації забезпечує захист інформації в інформаційно-телекомунікаційній системі надавача шляхом вирішення питань, пов'язаних з проектуванням, розробленням, модернізацією, введенням в експлуатацію та підтримкою працездатності комплексної системи захисту інформації, та додержання режиму безпеки в інформаційно-телекомунікаційній системі надавача.

6. Основними функціями служби захисту інформації є:

- 1) забезпечення повноти та якісного виконання організаційно-технічних заходів із захисту інформації;
- 2) розроблення розпорядчих документів, згідно з якими надавач повинен забезпечувати захист інформації, контроль за їх виконанням;
- 3) своєчасне реагування на спроби несанкціонованого доступу до інформаційних ресурсів інформаційно-телекомунікаційної системи надавача, порушення правил експлуатації засобів захисту інформації.

7. Керівник служби захисту інформації забезпечує належне виконання службою захисту інформації її функцій.

Фізичне середовище

1. Фізичний доступ до обладнання програмно-технічного комплексу, що забезпечує сертифікацію, управління статусом сертифіката, генерацію ключів надавача, повинен бути обмежений та надаватися тільки визначеному колу осіб із числа найманих працівників.

2. Надавачем повинно бути вжито запобіжних заходів щодо недопущення крадіжки, втрати та ушкодження обладнання, крадіжки та знищення (руйнування) інформації або інших дій, що можуть привести до виведення надавача із штатного режиму роботи.

3. Надавач повинен мати у власності або в користуванні спеціальні приміщення за його місцезнаходженням та місцезнаходженням його відокремлених пунктів реєстрації (за наявності).

Спеціальні 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 інвалідністю та інших маломобільних груп населення розміщується у місці, доступному для візуального сприйняття користувачів.

4. Спеціальні приміщення призначено для розташування технічних засобів, за допомогою яких здійснюється генерація та використання особистих ключів надавача, а також використання інформації, необхідність технічного захисту якої визначена у технічному завданні на створення комплексної системи захисту інформації або моделлю системи управління інформаційною безпекою надавача.

5. Шафи (сховища тощо), що призначені для зберігання технічних засобів та виготовлені в екранованому виконанні дозволяється розміщувати не в спеціальних приміщеннях із забезпеченням захисту від несанкціонованого доступу до них.

6. Технічний захист інформації, в тому числі захист від впливу зовнішніх електромагнітних полів, у спеціальних приміщеннях здійснюється шляхом створення умов щодо забезпечення електромагнітного екранування технічних засобів, а також шаф шляхом:

1) суцільного екранування усієї внутрішньої поверхні спеціальних приміщень;

2) розміщення технічних засобів та шаф в окремій екранованій кабіні (декількох кабінах);

3) розміщення у неекранованих спеціальних приміщеннях лише екранованих шаф і технічних засобів в екранованому виконанні;

4) погодження з контролюючим органом розміщення в неекранованих спеціальних приміщеннях технічних засобів та шаф за умови забезпечення захисту інформації від витоку каналами пасивного захисту інформації від її витоку каналами побічних електромагнітних випромінювань та наведень, а також порушення її цілісності внаслідок деструктивного впливу зовнішніх електромагнітних полів.

7. Для спеціальних приміщень рекомендується обирати приміщення, що відокремлені від зовнішніх стін (зі сторони оточуючої міської забудови)

коридорами тощо. Розміщення спеціальних приміщень під (над) санітарно-технічними кімнатами та гаражами не рекомендується.

8. Вікна спеціального приміщення повинні бути:

1) обладнані надійними металевими ґратами, якщо вони зовнішні та розташовані на першому чи останньому поверсі будівлі, або до яких можливе проникнення сторонніх осіб з дахів сусідніх будівель, із розташованих поруч пожежних сходів (труб водостоків тощо), а також якщо вони є внутрішніми і мають вихід до інших приміщень акредитованого центру;

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

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

9. Спеціальні приміщення повинні бути обладнані системою контролю доступу та пожежною сигналізацією. Двері спеціальних приміщень повинні бути обладнані кодовим замком або системою доступу.

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

11. Необхідна величина ефективності екранування та діапазон частот, у тому числі щодо рівня захищеності від витоку інформації каналами пасивного захисту інформації від її витоку каналами побічних електромагнітних випромінювань та наведень, повинні визначатися на етапі проектування та облаштування спеціальних приміщень залежно від достатності рівня захищеності технічних засобів від витоку інформації каналами пасивного захисту інформації від її витоку каналами побічних електромагнітних випромінювань та наведень.

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

13. Спеціальні екрановані приміщення (окрема екранована кабіна (шафа), технічні засоби в екранованому виконанні) повинні оснащуватися:

- 1) протизавадними фільтрами для захисту введів мереж електроживлення;
- 2) протизавадними фільтрами конструкції типу «поза межний хвильовід» для захисту місць вводу систем опалення, вентиляції і кондиціонування повітря;
- 3) іншими відповідними протизавадними фільтрами у разі необхідності введів оптоволоконних мереж, сигнальних тощо.

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

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

15. Для електроживлення технічних засобів, що розміщуються у спеціальних приміщеннях, спільно з протизавадними фільтрами захисту кіл електроживлення повинні бути встановлені пристрої безперервного електроживлення.

16. Система заземлення спеціальних приміщень та їх складових елементів не повинні утворювати замкнутих контурів, розміщуватися в межах контрольованої зони надавача чи у місцях із максимально ускладненим доступом до них сторонніх осіб, а також не повинні мати гальванічного зв'язку з металоконструкціями будівлі, іншими системами заземлення, екрануючими та захисними оболонками кабелів і з'єднувальних ліній, що мають вихід за межі контрольованої зони.

17. У разі об'єднання окремих технічних засобів, що розміщені у спеціальних приміщень, у локальну обчислювальну мережу, а також введення до спеціальних приміщень кабелів та ліній зв'язку, необхідно використовувати технології волоконно-оптичних ліній зв'язку та дотриманням пункту 11 цього підрозділу.

18. У разі, якщо за результатами спеціальних досліджень (атестації тощо) технічних засобів, розміщених у спеціальних приміщеннях, виявилось недостатнім впровадження визначених у цьому підрозділі заходів для забезпечення захищеності інформації від витоку інформації за рахунок пасивного захисту інформації від її витоку каналами побічних електромагнітних випромінювань та наведень, повинні бути впроваджені додаткові заходи з пасивного або активного захисту інформації.

Контроль доступу

1. Надавачем повинен бути передбачений захист внутрішньої обчислювальної мережі від несанкціонованого доступу з боку користувачів зовнішньої мережі (глобальних мереж), включаючи користувачів та третіх сторін. Засоби контролю доступу до інформаційних ресурсів надавача повинні відхиляти всі мережеві протоколи та спроби доступу, що необов'язкові для функціонування інформаційно-телекомунікаційної системи надавача.

2. Надавачем повинно бути реалізовано адміністрування з метою розмежування доступу найманих працівників надавача до ресурсів системи та надання функцій тільки згідно з авторизацією найманого працівника надавача можливості виконувати тільки ті функції, що доступні та асоційовані з їх функціями та завданнями).

3. Найманий працівник надавача повинен бути успішно ідентифікований та автентифікований перед початком виконання процедур, пов'язаних із формуванням сертифіката або зміною його статусу.

4. Всі дії найманих працівників надавача, пов'язані із генерацією пар ключів, формуванням сертифіката або зміною його статусу, повинні протоколюватися із забезпеченням захисту протоколів від несанкціонованого доступу.

5. Резервні копії сертифікатів відкритих ключів та журналів аудиту подій повинні зберігатися в окремому приміщенні надавача із забезпеченням їх захисту від несанкціонованого доступу.

6. Програмно-технічний комплекс повинен забезпечувати реєстрацію дій найманих працівників надавача. Журнали аудиту подій повинні мати захист від несанкціонованого доступу, модифікації або знищення (руйнування) інформації.

Криптографічний контроль

1. Для надання кваліфікованих електронних довірчих послуг надавач повинен використовувати засоби кваліфікованого електронного підпису чи печатки.

2. Всі засоби кваліфікованого електронного підпису чи печатки, пари особистих та відкритих ключів надавача, а також їх резервні копії мають бути обліковані адміністратором безпеки.

3. У своїй діяльності надавач використовує тільки криптографічні алгоритми з належним рівнем стійкості. Перелік криптографічних алгоритмів дозволених для використання при наданні електронних довірчих послуг визначається регламентом роботи центрального засвідчувального органу.

Операційна безпека

1. Надавач у інформаційно-телекомунікаційній системі використовує загальносистемні технічні та програмні засоби, що мають вбудовані функції контролю цілісності, автентифікації користувачів, ведення журналів подій, безпечного виконання операцій тощо. Перевага надається технічним та програмним засобам, що мають позитивний експертний висновок за результатами державної експертизи у галузі технічного захисту інформації.

2. Надавач використовує технічні та програмні засоби з дотриманням ліцензійної угоди виробника такого засобу.

3. Всі технічні засоби інформаційно телекомунікаційної системи надавача обліковуються, а зміни їх складі документуються.

4. Інформаційно-телекомунікаційна система надавача має бути захищена від вірусного, зловмисного та неавторизованого програмного забезпечення.

5. Надавачем має здійснюватися контроль використання носіїв інформації, в тому числі запобігання від несанкціонованого підключення зовнішніх носіїв інформації, викрадення, пошкодження, фізичного застарівання та несанкціонованого доступу до носіїв інформації.

6. Надавачем здійснюється регулярне встановлення оновлень безпеки для технічних та програмних засобів. Якщо оновлення безпеки несе потенційно більшу шкоду або не застосовується з іншої причини, посадовими особами надавача складається відповідний акт.

Мережева безпека

1. Надавач використовує для захисту своєї інформаційно-телекомунікаційну систему засоби захисту від кібератак.

2. Заходи від захисту від кібератак включають розподілення мережі інформаційно-телекомунікаційної системи на сегменти на основі оцінки ризику з урахуванням функціональної, логічної та фізичної (включаючи місцезнаходження) взаємозв'язку між надійними системами та службами. До всіх засобів розташованих у тому самому сегменті застосовуються однакові елементи контролю безпеки. Доступи і зв'язки між сегментами обмежуються тільки необхідними для правильного функціонування інформаційно-телекомунікаційної системи, а необов'язкові підключення та служби повинні бути явно заборонені або дезактивовані.

3. Локальний сегмент мережі, що використовується для управління інформаційно-телекомунікаційною системою та операційний сегмент мережі, через який здійснюється обслуговування підписувачів надавача, повинні бути розділені. Робочі станції адміністраторів безпеки та системи, що використовуються для управління інформаційною безпекою, не повинні використовуватися для інших цілей. Інформаційно-телекомунікаційна система надавача має бути відокремлена від середовищ розробки та тестування.

4. Конфіденційна інформація та персональні дані користувача, що надаються під час реєстрації користувача, повинні бути належним чином захищені у разі їх передавання зовнішніми комп'ютерними мережами.

5. Для інформаційно-телекомунікаційної системи надавача повинно здійснюватися регулярне сканування вразливостей на загальнодоступній та приватній (за наявності) зовнішніх мережевих адресах. На етапі введення інформаційно-телекомунікаційної системи надавача в експлуатацію або, за

необхідності, після проведення її модернізації повинен бути здійснено тестування на проникнення.

6. Факт проведення сканування вразливостей або тестування на проникнення документується із зазначенням доказів того, що кожне таке сканування вразливостей або тест на проникнення виконувалися фізичною особою чи юридичною особою з навичками, інструментами, вмінням, етичним кодексом та незалежністю, необхідними для надання достовірного звіту.

Управління інцидентами

1. З метою забезпечення ефективного управління в інформаційно-телекомунікаційній системі надавача здійснюється функціонування системи моніторингу, що збирає та аналізує інформацію про стан критичних компонентів інформаційно-телекомунікаційної системи, в тому числі про вимкнення, запуск, перезапуск, доступність та рівень навантаження таких компонентів.

2. Система моніторингу має виявляти та повідомляти сигналом тривоги аномальну системну активність, що вказує на потенційне порушення системи безпеки, включаючи вторгнення в інформаційно-телекомунікаційну систему.

3. Здійснення заходів реагування на потенційно критичні інциденти покладено на службу захисту інформації надавача, яка повинна діяти своєчасно та скоординовано, щоб швидко реагувати на інциденти та обмежити вплив порушень безпеки.

4. Надавач повинен встановити порядок повідомлення контролюючого органу щодо будь-якого порушення безпеки або втрати цілісності даних, що суттєво впливає на електронну довірчу послугу та на персональні дані, що зберігаються в ній, протягом 24 годин після виявлення порушення.

5. Якщо є підстави вважати, що порушення безпеки або втрата цілісності даних спричинить негативний вплив на фізичну або юридичну особу, якій надавалася електронна довірча послуга, надавач повинен негайно повідомити таку фізичну або юридичну особу.

6. Надавачем повинен бути розроблений та затверджений керівником надавача порядок (план) безперервної роботи, що визначатиме порядок дій при виникненні критичних ситуацій, включаючи стихійні лиха та компрометацію особистих ключів.

Журнали аудиту

1. З метою забезпечення збереження інформації про всі дії та події, що відбуваються в інформаційно-телекомунікаційній системі надавача ведуться журнали аудиту подій.

2. У журналах аудиту подій реєструються дії та події таких типів:

1) спроби створення, знищення, встановлення паролів, зміни прав доступу в інформаційно-телекомунікаційній системі надавача тощо;

2) заміни технічних засобів інформаційно-телекомунікаційної системи надавача та пар ключів;

3) формування, блокування, скасування та поновлення сертифікатів ключів, формування списків відкликаних сертифікатів відкритих ключів;

4) спроби несанкціонованого доступу до інформаційно-телекомунікаційної системи надавача;

5) надання доступу персоналу до інформаційно-телекомунікаційної системи надавача;

6) зміна системних конфігурацій та технічне обслуговування інформаційно-телекомунікаційної системи надавача;

7) збоїв в роботі інформаційно-телекомунікаційної системи надавача;

8) інші події, відомості про які фіксуються в журналі аудиту подій.

3. Усі записи в журналах аудиту подій в електронній або паперовій формі повинні містити дату та час дії або події, а також ідентифікувати суб'єкта, що її здійснив або ініціював.

4. Журнали аудиту подій підлягають перегляду не рідше одного разу на тиждень.

Перегляд передбачає перевірку того, що журнал аудиту подій не піддавався несанкціонованим модифікаціям, вивчення всіх дій та/або подій у журналі аудиту подій з приділенням особливої уваги повідомленням про невідповідності і попередженням про небезпечні ситуації.

Перегляд журналів аудиту подій здійснює адміністратор аудиту.

5. Система ведення електронного журналу аудиту подій повинна бути синхронізована із Всесвітнім координованим часом з точністю до секунди та включати механізми його захисту від неавторизованого перегляду, модифікації і знищення.

Записи подій у журналах аудиту подій в паперовій формі повинні бути завірені і підписані адміністратором безпеки.

Журнали аудиту подій в електронній формі резервуються з періодичністю не менше одного разу на тиждень.

6. Надавач зберігає журнали аудиту подій на місці їх створення протягом 10 років, після чого забезпечує їх передачу для архівного зберігання.

Операційний контроль

1. Генерація пари ключів надавача здійснюється адміністратором сертифікації під контролем адміністратора безпеки та, у разі необхідності, за участю інших посадових осіб надавача, визначених рішенням керівника.

Генерація пари ключів надавача здійснюється за допомогою засобів кваліфікованого електронного підпису чи печатки.

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

3. Особистий ключ надавача повинен розміщуватися на захищеному носії особистого ключа в складі програмно-апаратного або апаратного засобу криптографічного захисту інформації, яким здійснювалася генерація пари ключів.

Технологія зберігання особистого ключа надавача повинна забезпечити неможливість доступу до нього ззовні у відношенні до засобу криптографічного захисту інформації.

4. У разі здійснення резервування особистий ключ надавача повинен бути перенесений на зовнішній носій (пристрій) у захищеному вигляді, що забезпечує його цілісність та конфіденційність.

Резервування та відновлення особистого ключа надавача здійснюється адміністратором сертифікації під контролем адміністратора безпеки та, у разі необхідності, за участю інших посадових осіб надавача, визначених рішенням керівника.

5. Умови забезпечення захисту резервної копії особистого ключа надавача під час його зберігання повинні бути не нижче, ніж умови забезпечення захисту особистого ключа, що знаходиться у використанні.

6. Особистий ключ надавача може використовуватися лише 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.

7. Особистий ключ надавача може використовуватися лише у засобах криптографічного захисту інформації, які повинні бути розташовані у окремому спеціально призначеному для цього приміщенні.

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

5. Вимоги до регламенту роботи надавача

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

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

3. У регламенті роботи надавача повинно бути визначено:

1) загальні положення (ідентифікаційні дані надавача – найменування, код за Єдиним державним реєстром підприємств та організацій України, місцезнаходження, номери телефонів, електронна адреса веб-сайту);

2) перелік відокремлених пунктів реєстрації (за наявності), їх місцезнаходження, номери телефонів;

3) посадовий та персональний склад надавача, функції посадових осіб надавача;

4) політика сертифіката та положення сертифікаційних практик.

4. Політики сертифіката можуть описувати кожну кваліфіковану послугу, що надається надавачем окремо або у сукупності.

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

5. 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 підписувачем особистим ключем, відповідний якому відкритий ключ надається для сертифікації;

б) умови встановлення фізичної особи або представника юридичної особи (інформація, що надається заявником під час реєстрації, види документів, на підставі яких встановлюється заявник, вимоги щодо особистої присутності);

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

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

4) управління та операційний контроль:

а) фізичне середовище (опис спеціального приміщення, механізми контролю доступу до нього);

б) процедурний контроль (перелік посад безпосередньо задіяних в обслуговуванні кваліфікованих сертифікатів відкритих ключів, їх функції та відповідальність 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 надання особистого ключа користувачу після його генерації надавачем;

в) механізм надання відкритого ключа користувача надавачу для сертифікації;

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.

6. 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 сертифікацію (перелік суб'єктів, уповноважених здійснювати запит на сертифікацію, порядок подачі та оброблення запиту на сертифікацію, строки оброблення запиту на сертифікацію);

2) надання сформованого кваліфікованого сертифіката відкритого ключа заявнику;

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

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

5) процедура подачі запиту на сертифікацію для заявників, 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;

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

Після погодження контролюючим органом регламент роботи надавача затверджується його керівником у двох примірниках, один з яких передається до контролюючого органу.

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

9. Надавач забезпечує ознайомлення користувачів з положеннями регламенту його роботи та іншими документами, відповідно до яких надаються кваліфіковані електронні довірчі послуги, шляхом розміщення відповідних документів та інформації на своєму офіційному веб-сайті.

6. Вимоги до початку роботи надавача

1. Для набуття статусу надавача заявник подає до центрального засвідчувального органу:

1) документи визначені частиною другою статті 30 Закону України «Про електронні довірчі послуги»;

2) одну або декілька заяв та відповідних їм електронних запитів на формування кваліфікованого сертифіката відкритого ключа електронних

довірчих послуг заявника, що формуються за результатами генерації пар (особистого та відкритого) ключів таких послуг (за необхідністю);

3) підписаний примірник договору про надання центральним засвідчувальним органом кваліфікованої електронної довірчої послуги формування, перевірки та підтвердження чинності кваліфікованого сертифіката електронного підпису чи печатки для кожної послуги (за необхідністю).

2. Заявник набуває статусу надавача з дня внесення відомостей про нього та про кваліфіковані електронні довірчі послуги, які він надає, до Довірчого списку на підставі рішення центрального засвідчувального органу, прийнятого за результатами розгляду заяви про внесення до Довірчого списку, за формою, встановленою у регламенті роботи центрального засвідчувального органу, а також документів передбачених статтею 30 Закону України «Про електронні довірчі послуги».

3. Заява про внесення до Довірчого списку та документи, що до неї додаються, можуть бути подані заявником в електронній формі через Єдиний державний портал адміністративних послуг, у тому числі через інтегровану з ним інформаційну систему центрального засвідчувального органу, із застосування кваліфікованого електронного підпису заявника.

Копії документів, які існують тільки в паперовій формі, додаються до заяви про внесення до Довірчого списку у форматі PDF.

Відповідність оригіналам копій документів, передбачених частиною другою статті 30 Закону України «Про електронні довірчі послуги», засвідчується шляхом накладення кваліфікованого електронного підпису заявника – фізичної особи – підприємця або керівника заявника – юридичної особи.

Заявник відповідає за достовірність інформації наданої в документах для внесення до Довірчого списку.

У разі подання заяви про внесення 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).

Під час надходження електронні документи реєструються в системі центрального засвідчувального органу, про що автоматично інформується заявник через персональний кабінет на Єдиному державному порталі адміністративних послуг.

Центральний засвідчувальний орган здійснює розгляд заяви про внесення до Довірчого списку та документів, що до неї додаються, і за результатами їх розгляду приймає рішення у порядку та строки, встановлені Законом України «Про електронні довірчі послуги».

Центральний засвідчувальний орган повідомляє заявника про прийняте рішення в електронній формі через персональний кабінет на Єдиному державному порталі адміністративних послуг, а також оприлюднює таке рішення на офіційному веб-сайті центрального засвідчувального органу.

Електронні документи зберігаються відповідно до Закону України «Про електронні документи та електронний документообіг».

4. На підставі прийнятого рішення щодо внесення відомостей про надавача до Довірчого списку центральний засвідчувальний орган засвідчує один або декілька відкритих ключів кваліфікованих електронних довірчих послуг надавача.

5. Зміна відомостей про надавача або про кваліфіковані електронні довірчі послуги, які він надає, внесених до Довірчого списку, є підставою для внесення змін до Довірчого списку.

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. Сформований центральним засвідчувальним органом кваліфікований сертифікат відкритого ключа кваліфікованої електронної довірчої послуги надавача має строк чинності відповідно до регламенту роботи центрального засвідчувального органу.

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 лише 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. Надання кваліфікованої електронної довірчої послуги передбачає:

1) реєстрацію користувача;

2) генерацію пари ключів користувача;

3) сертифікацію користувача;

4) публікацію кваліфікованого сертифіката відкритого ключа;

5) постійне зберігання кваліфікованого сертифіката відкритого ключа та документів, на основі яких було здійснено сертифікацію користувача;

6) цілодобовий доступ до реєстру чинних, блокованих та скасованих сертифікатів відкритих ключів та до інформації про статус кваліфікованого сертифіката відкритого ключа;

7) цілодобовий прийом заяв користувача з питань скасування, блокування та поновлення його кваліфікованого сертифіката відкритого ключа;

8) унеможливлення використання особистого ключа користувача в разі його компрометації;

9) інформування надавачем про всі випадки порушення конфіденційності та/або цілісності інформації;

10) надання користувачу у користування засобу кваліфікованого електронного підпису чи печатки, його технічну підтримку та обслуговування.

4. Під час реєстрації користувача адміністратором реєстрації здійснюється ідентифікація заявника шляхом перевірки ідентифікаційних даних з документів, що надаються заявником, та даних одержаних з інформаційних систем органів державної влади.

5. Ідентифікація заявника – фізичної особи, представника юридичної особи, перевірка його цивільної правоздатності та дієздатності здійснюється відповідно до вимог статті 22 Закону України «Про електронні довірчі послуги».

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

- 1) за умови особистої присутності заявника;
- 2) віддалено, з використанням засобу електронної ідентифікації заявника, що підпадає під високий рівень довіри до схеми електронної ідентифікації, затвердженої Кабінетом Міністрів України, який було отримано заявником за умови його особистої присутності;
- 3) шляхом використання ідентифікаційних даних з чинного кваліфікованого сертифіката відкритого ключа, сформованого тим самим надавачем.

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

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

9. У разі, якщо надання кваліфікованої електронної довірчої послуги передбачає генерацію пари ключів користувача, персоналом надавача забезпечується створення умов для генерації пари ключів, та, в разі необхідності, користувачу надається допомога під час генерації пари ключів у спосіб, що не допускає порушення конфіденційності та цілісності ключа, а також ознайомлення із значенням параметрів особистих ключів та їх копіювання.

Допускається реєстрація користувача у разі, якщо пара ключів була згенерована заявником поза спеціальним приміщенням надавача та за відсутності відповідного персоналу, шляхом забезпечення адміністратором реєстрації перевірки володіння заявником особистим ключем, який відповідає відкритому ключу, наданому для формування кваліфікованого сертифіката відкритого ключа.

Перевірка володіння заявником особистим ключем виконується без розкриття особистого ключа такого заявника.

10. Умови для генерації пари ключів повинні передбачати заходи із забезпечення конфіденційності під час генерації пари ключів користувача.

11. Генерація пари ключів користувача здійснюється за допомогою засобу кваліфікованого електронного підпису чи печатки з дотриманням вимог щодо забезпечення:

- 1) належного рівня унікальності пари ключів, що ним генерується;
- 2) конфіденційності особистих ключів під час їх генерації, зберігання та створення кваліфікованого електронного підпису чи печатки;
- 3) захисту від доступу до особистих ключів сторонніх осіб.

12. Зберігання особистого ключа користувача та ознайомлення з ним надавача забороняються.

13. Сертифікація користувача передбачає формування кваліфікованого сертифіката відкритого ключа та повторне формування кваліфікованого

сертифіката відкритого ключа користувача адміністратором реєстрації на підставі ідентифікаційних даних, одержаних від заявника під час реєстрації користувача.

14. Надавач повинен забезпечити унікальність розпізнавального імені користувача та серійного номера кваліфікованого сертифіката відкритого ключа серед інших кваліфікованих сертифікатів відкритих ключів, сформованих цим самим надавачем.

15. Надавачем повинна забезпечуватись можливість резервування усіх сформованих ним кваліфікованих сертифікатів відкритих ключів.

16. Під час повторного формування кваліфікованого сертифіката відкритого ключа надавач повинен здійснити перевірку актуальності інформації, що надавалась для попередньої реєстрації користувача.

17. Кваліфікований сертифікат відкритого ключа після його формування Надавачем повинен бути доступний користувачу, для якого цей кваліфікований сертифікат відкритого ключа був сформований.

18. Доступ інших осіб до сформованого кваліфікованого сертифіката відкритого ключа надається у разі згоди користувача на публікацію його кваліфікованого сертифіката відкритого ключа.

19. У разі необхідності внесення змін до даних, що містяться у кваліфікованому сертифікаті відкритого ключа користувача, надавач може здійснити повторну публікацію кваліфікованого сертифіката відкритого ключа із використанням засвідченого раніше відкритого ключа користувача, якщо відповідний йому особистий ключ не був скомпрометований.

Під час повторної публікації кваліфікованого сертифіката відкритого ключа надавачем повинні бути дотримані вимоги, що встановлені для реєстрації користувача.

Повторна публікація кваліфікованого сертифіката відкритого ключа не продовжує строку його дії.

20. Сформований кваліфікований сертифікат відкритого ключа користувача скасовується або блокується надавачем у разі надходження до нього відповідної заяви користувача.

21. Під час опрацювання заяви користувача про скасування або блокування кваліфікованого сертифіката відкритого ключа адміністратором сертифікації здійснюється ідентифікація заявника з дотриманням вимог щодо підтвердження особи, встановлених у регламенті роботи надавача.

22. Кваліфікований сертифікат відкритого ключа вважається скасованим або блокованим з моменту зміни надавачем статусу кваліфікованого сертифіката відкритого ключа на скасований або блокований.

23. Користувач, статус кваліфікованого сертифіката відкритого ключа якого було змінено на скасований чи блокований, повинен бути поінформований про відповідну зміну статусу.

24. Скасований кваліфікований сертифікат відкритого ключа поновленню не підлягає.

25. Відомості про сертифікати відкритих ключів, сформовані надавачем, їх статус та списки відкликаних сертифікатів відкритих ключів містяться у реєстрі чинних, блокованих та скасованих сертифікатів відкритих ключів.

26. Розповсюдження інформації про статус кваліфікованих сертифікатів відкритих ключів користувачів здійснюється за допомогою публікації повного та часткового списків відкликаних сертифікатів на офіційному веб-сайті надавача та забезпечення можливості перевірки статусу кваліфікованого сертифіката відкритого ключа користувача в режимі реального часу через телекомунікаційні мережі загального користування.

Вимоги до формату списку відкликаних сертифікатів встановлюються головним органом у системі центральних органів виконавчої влади, що забезпечує формування та реалізує державну політику у сфері електронних довірчих послуг спільно зі спеціально уповноваженим центральним органом виконавчої влади з питань організації спеціального зв'язку та захисту інформації.

До списку відкликаних сертифікатів надавача висуваються такі вимоги:

1) кожен список відкликаних сертифікатів повинен містити час видання наступного списку, якщо інше не передбачено регламентом роботи надавача;

2) новий список відкликаних сертифікатів може бути опублікований до визначеного часу видання наступного списку;

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

27. Управління статусом кваліфікованого сертифіката відкритого ключа та розповсюдження інформації про статус кваліфікованого сертифіката відкритого ключа повинні бути доступні для користувача цілодобово.

28. Заяви про скасування або блокування кваліфікованого сертифіката відкритого ключа фіксуються та зберігаються надавачем.

29. Надавач повинен забезпечити цілісність та автентичність інформації про статус кваліфікованих сертифікатів відкритих ключів.

30. Час, що використовується надавачем в процесі обслуговування кваліфікованих сертифікатів відкритих ключів користувачів, повинен бути синхронізований з Всесвітнім координованим часом (UTC) з точністю до секунди.

31. Обслуговування кваліфікованих сертифікатів відкритих ключів надавачів здійснюється центральним засвідчувальним органом відповідно до

регламенту роботи центрального засвідчувального органу з дотриманням цих Вимог.

32. Надавач повинен забезпечити можливість ознайомлення користувачів з інформацією про умови отримання кваліфікованої електронної довірчої послуги та використання кваліфікованого сертифіката відкритого ключа, сформованого на основі такої послуги.

До інформації, вільний доступ до якої повинен забезпечити надавач, відноситься:

- 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) 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.

33. Інформація про умови отримання кваліфікованої електронної довірчої послуги та використання кваліфікованого сертифіката відкритого ключа, сформованого на основі такої послуги, надається користувачам, у тому числі, шляхом її розміщення на офіційному веб-сайті надавача.

34. Інформація на офіційному веб-сайті надавача повинна бути доступною для осіб з обмеженими фізичними можливостями, зокрема для користувачів з вадами зору та слуху.

35. Кваліфіковані електронні довірчі послуги надаються надавачем на підставі заяви та договору про надання кваліфікованої електронної довірчої послуги.

В органах державної влади, органах місцевого самоврядування, підприємствах, установах та організаціях державної форми власності

кваліфіковані електронні довірчі послуги можуть надаватися на підставі інших документів.

Форми заяви та договору про надання кваліфікованої електронної довірчої послуги встановлюються головним органом у системі центральних органів виконавчої влади, що забезпечує формування та реалізує державну політику у сфері електронних довірчих послуг.

36. Надавач бере на облік договори про надання кваліфікованих електронних довірчих послуг, а також документи (засвідчені в установленому порядку копії документів), що використовуються під час реєстрації користувача.

37. Договір про надання кваліфікованих електронних довірчих послуг повинен містити:

- 1) обов'язки сторін, у тому числі щодо обов'язковості використання засобів кваліфікованого електронного підпису чи печатки;
- 2) умови використання користувачем особистого ключа;
- 3) умови надання доступу користувачам до сертифіката підписувача (умови публікації сертифіката).
- 4) строк дії;
- 5) умови та оплати;
- 6) підстави для внесення змін або розірвання договору про надання кваліфікованої електронної довірчої послуги;
- 7) відомості про згоду або незгоду користувача надавати вільний доступ до його кваліфікованого сертифіката відкритого ключа іншим особам;
- 8) порядок взаємодії користувача з надавачем.

38. Договір про надання кваліфікованої електронної довірчої послуги може бути змінено лише на підставі взаємної згоди сторін.

39. У разі зміни відомостей, що містяться у договорі про надання кваліфікованої електронної довірчої послуги та/або кваліфікованому сертифікаті відкритого ключа, сформованому на підставі такого договору, користувач у триденний строк з дня настання таких змін повідомляє про це надавача.

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

- 1) згода сторін;
- 2) рішення суду на вимогу однієї із сторін у разі істотного порушення договору другою стороною;
- 3) виключення надавача з Довірчого списку.

41. У разі розірвання договору про надання кваліфікованої електронної довірчої послуги кваліфікований сертифікат відкритого ключа, сформований на підставі такого договору, скасовується.

42. Під час надання кваліфікованих електронних довірчих послуг надавач виконує обов'язки передбачені частиною другою статті 13 Закону України «Про електронні довірчі послуги».

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

1. Кваліфікована електронна довірча послуга створення, перевірки та підтвердження кваліфікованих електронних підписів чи печаток передбачає:

1) надання користувачам передбачених частиною першою статті 18 Закону України «Про електронні довірчі послуги» в тому числі і дистанційним способом;

2) використання лише засобів кваліфікованого електронного підпису чи печатки та кваліфікованих сертифікатів електронного підпису чи печатки;

3) дотримання належного рівня захисту обміну інформації між користувачем та надавачем засобами телекомунікаційних мереж.

2. Створення кваліфікованих електронних підписів чи печаток здійснюється надавачем за запитом користувача.

3. Засоби кваліфікованого електронного підпису чи печатки, що використовуються для створення кваліфікованих електронних підписів чи печаток, повинні задовольняти щонайменше наступним вимогам:

1) забезпечено належний рівень конфіденційності даних створення електронного підпису чи печатки;

2) забезпечено належний рівень унікальності даних створення електронного підпису чи печатки;

3) забезпечено належний рівень захисту даних створення електронного підпису чи печатки від підробки, використовуючи наявні технології;

4) дані створення електронного підпису чи печатки можуть бути захищені від використання іншими особами користувачем.

4. Засоби кваліфікованого електронного підпису чи печатки, що використовуються для створення кваліфікованих електронних підписів чи печаток, не повинні змінювати дані, для яких створюється кваліфікований електронний підпис чи печатка, або забороняти надання таких даних користувачу перед підписанням.

5. Створення або керування даними створення електронного підпису чи печатки від імені користувача може здійснювати лише надавач.

6. Надавачі, які керують даними створення кваліфікованого електронного підпису чи печатки від імені користувача, можуть здійснювати дублювання зазначених даних лише для цілей резервування, якщо це не суперечить підпункту 4 пункту 3 цього розділу та за умови дотримання таких вимог:

1) безпека дубльованих даних повинна бути такою ж, як і для вихідних наборів даних;

2) обсяг дубльованих даних не повинен перевищувати мінімального значення, що необхідне для забезпечення безперервності послуги.

7. Кваліфікований електронний підпис чи печатка вважається таким, що пройшов перевірку та отримав підтвердження, якщо:

1) виконуються вимоги частини другої статті 18 Закону України «Про електронні довірчі послуги»;

2) ідентифікаційні дані підписувача чи створювача електронної печатки до відповідного кваліфікованого сертифіката електронного підпису чи печатки було внесено вірно;

3) під час перевірки було встановлено, що кваліфікований електронний підпис чи печатка було створено за допомогою засобу кваліфікованого електронного підпису чи печатки.

8. Перевірка кваліфікованого електронного підпису чи печатки може здійснюватися будь-якою особою з метою отримання інформації про дійсність чи недійсність кваліфікованого електронного підпису чи печатки за допомогою кваліфікованого сертифіката відкритого ключа підписувача чи створювача кваліфікованої електронної печатки, а також надавача самостійно (без взаємодії з надавачем).

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

1) послуга надається лише надавачем;

2) послуга відповідає всім вимогам до перевірки кваліфікованих електронних підписів чи печаток, зазначеним у пункті 7 цього розділу;

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

10. Контроль за наданням кваліфікованої електронної довірчої послуги створення, перевірки та підтвердження кваліфікованих електронних підписів чи печаток надавачами здійснює контролюючий орган.

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

1. Кваліфікована електронна довірча послуга формування, перевірки та підтвердження чинності кваліфікованого сертифіката електронного підпису чи печатки передбачає надання користувачам передбачених частиною першою статті 20 Закону України «Про електронні довірчі послуги».

2. Надавачем кваліфікованої електронної довірчої послуги формування, перевірки та підтвердження чинності кваліфікованого сертифіката електронного підпису чи печатки окремо чи у сукупності застосовуються наступні політики сертифіката відповідно до національного стандарту ДСТУ ETSI EN 319 411-2:2016 (ETSI EN 319 411-2:2016, IDT) «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»:

1) політика кваліфікованого сертифіката відкритого ключа електронного підпису, виданого фізичній особі (QCP-n);

2) політика кваліфікованого сертифіката відкритого ключа електронної печатки, виданого юридичній особі (QCP-l);

3) політика кваліфікованого сертифіката відкритого ключа електронного підпису, виданого фізичній особі, відповідний особистий ключ якого зберігається у засобі кваліфікованого електронного підпису чи печатки, який має вбудовані апаратно-програмні засоби, що забезпечують захист записаних на них даних від несанкціонованого доступу, від безпосереднього ознайомлення із значенням параметрів особистих ключів та їх копіювання (QCP-n-QSCD);

4) політика кваліфікованого сертифіката відкритого ключа електронного підпису, виданого юридичній особі, відповідний особистий ключ якого зберігається у засобі кваліфікованого електронного підпису чи печатки, який має вбудовані апаратно-програмні засоби, що забезпечують захист записаних на них даних від несанкціонованого доступу, від безпосереднього ознайомлення із значенням параметрів особистих ключів та їх копіювання (QCP-l-QSCD).

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

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

5. Контроль за наданням кваліфікованої електронної довірчої послуги формування, перевірки та підтвердження чинності кваліфікованого сертифіката електронного підпису чи печатки надавачами здійснює контролюючий орган.

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

1. Кваліфікована електронна довірча послуга формування, перевірки та підтвердження чинності кваліфікованого сертифіката автентифікації веб-сайту передбачає надання користувачам передбачених частиною першою статті 21 Закону України «Про електронні довірчі послуги»..

2. Надавачем кваліфікованої електронної довірчої послуги формування, перевірки та підтвердження чинності кваліфікованого сертифіката автентифікації веб-сайту відповідно до національного стандарту ДСТУ ETSI EN 319 411-2:2016 (ETSI EN 319 411-2:2016, IDT) «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» застосовується політика кваліфікованого сертифіката відкритого ключа веб-сайта (QCP-w).

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

4. 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;

5. Перевірка кваліфікованого сертифіката автентифікації веб-сайту може здійснюватися будь-якою особою з метою отримання інформації про дійсність чи недійсність кваліфікованого сертифіката автентифікації веб-сайту за допомогою кваліфікованого сертифіката відкритого ключа надавача самостійно (без взаємодії з надавачем).

6. 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, 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.

7. Кваліфікований сертифікат автентифікації веб-сайту вважається недійсним 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.

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

9. Контроль за наданням кваліфікованої електронної довірчої послуги формування, перевірки та підтвердження чинності кваліфікованого сертифіката автентифікації веб-сайту надавачами здійснює контролюючий орган.

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

1. Кваліфікована електронна довірча послуга формування, перевірки та підтвердження кваліфікованої електронної позначки часу передбачає:

1) формування кваліфікованої електронної позначки часу;

2) передачу кваліфікованої електронної позначки часу користувачеві.

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

3. Під час формування кваліфікованої електронної позначки часу користувач та надавач 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;

б) 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.

4. 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.

5. Перевірка кваліфікованої електронної позначки часу може здійснюватися будь-якою особою з метою отримання інформації про дійсність чи недійсність кваліфікованої електронної позначки часу за допомогою кваліфікованого сертифіката відкритого ключа надавача самостійно (без взаємодії з надавачем).

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

1) отримує з кваліфікованої електронної позначки часу інформацію, що містить ідентифікаційні дані, 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).

7. 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.

8. Правильність реалізації криптографічних алгоритмів для створення кваліфікованої електронної позначки часу та точність часу в засобі кваліфікованого електронного підпису чи печатки забезпечує протокол фіксування часу.

Вимоги до протоколу фіксування часу встановлюються головним органом у системі центральних органів виконавчої влади, що забезпечує формування та реалізує державну політику у сфері електронних довірчих послуг спільно зі спеціально уповноваженим центральним органом виконавчої влади з питань організації спеціального зв'язку та захисту інформації.

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

10. 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.

11. Контроль за наданням кваліфікованої електронної довірчої послуги формування, перевірки та підтвердження кваліфікованої електронної позначки часу надавачами здійснює контролюючий орган.

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

1. Кваліфікована електронна довірча послуга реєстрованої електронної доставки передбачає:

- 1) відправку електронних даних;
- 2) отримання електронних даних.

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

3. Під час реєстрованої електронної доставки користувачі (відправник та отримувач електронних даних) та надавач виконують такі дії:

- 1) надаватися одним чи кількома надавачами;
- 2) повинна забезпечуватись електронна ідентифікація відправника;
- 3) перед доставкою електронних даних повинна забезпечуватись електронна ідентифікація отримувача;
- 4) до електронних даних, що відправляються, додається створений для них удосконалений електронний підпис чи удосконалена електронна печатка надавача;
- 5) відправник і отримувач електронних даних повинні бути повідомлені про будь-яку зміну електронних даних, необхідну для відправки або отримання цих даних;
- 6) дата і час відправки, отримання та будь-яка зміна електронних даних повинні фіксуватися з використанням кваліфікованої електронної позначки часу;
- 7) у разі відправки електронних даних між двома або більше надавачами наведені вище вимоги повинні застосовуватися до всіх надавачів.

4. 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.

5. Перевірка електронних даних, що передаються в процесі реєстрованої електронної доставки, здійснюється отримувачем електронних даних шляхом перевірки чинності кваліфікованого сертифіката відкритого ключа надавача самостійно (без взаємодії з надавачем).

6. Контроль за наданням кваліфікованої електронної довірчої послуги реєстрованої електронної доставки надавачами здійснює контролюючий орган.

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

1. Кваліфікована електронна довірча послуга зберігання кваліфікованих електронних підписів, печаток, електронних позначок часу та сертифікатів, пов'язаних з цими послугами, передбачає:

- 1) передачу кваліфікованих електронних підписів чи печаток та сформованих сертифікатів, пов'язаних з цими послугами;
- 2) зберігання кваліфікованих електронних підписів чи печаток та сформованих сертифікатів, пов'язаних з цими послугами.

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

3. 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.

4. Контроль за наданням кваліфікованої електронної довірчої послуги зберігання кваліфікованих електронних підписів, печаток, електронних позначок часу та сертифікатів, пов'язаних з цими послугами, надавачами здійснює контролюючий орган.

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. Технічні специфікації формату кваліфікованого сертифіката відкритого ключа встановлюються головним органом у системі центральних органів виконавчої влади, що забезпечує формування та реалізує державну політику у сфері електронних довірчих послуг, спільно зі спеціально уповноваженим центральним органом виконавчої влади з питань організації спеціального зв'язку та захисту інформації.

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