



АДМІНІСТРАЦІЯ ДЕРЖАВНОЇ СЛУЖБИ СПЕЦІАЛЬНОГО ЗВ'ЯЗКУ
ТА ЗАХИСТУ ІНФОРМАЦІЇ УКРАЇНИ

НАКАЗ

24.07.2007 N 143

Зареєстровано в Міністерстві
юстиції України
8 серпня 2007 р.
за N 914/14181

Про затвердження Положення про порядок
здійснення державного контролю за додержанням
вимог законодавства у сфері надання послуг
електронного цифрового підпису

Відповідно до Законів України "Про електронний цифровий підпис" ([852-15](#)), "Про Державну службу спеціального зв'язку та захисту інформації України" ([3475-15](#)), Положення про Адміністрацію Державної служби спеціального зв'язку та захисту інформації, затвердженого постановою Кабінету Міністрів України від [24.06.2006](#) N 868 ([868-2006-п](#)), з метою здійснення державного контролю за додержанням законодавства у сфері електронного цифрового підпису **НАКАЗУЮ**:

1. Затвердити Положення про порядок здійснення державного контролю за додержанням вимог законодавства у сфері надання послуг електронного цифрового підпису, що додається.

2. Начальнику Департаменту регулювання діяльності у сфері криптографічного захисту інформації забезпечити подання в установленому порядку цього наказу на державну реєстрацію до Міністерства юстиції України.

3. Контроль за виконанням цього наказу покласти на першого заступника Голови Державної служби спеціального зв'язку та захисту інформації України.

Т.в.о Голови Служби

О.І.Сиров

ЗАТВЕРДЖЕНО
Наказ Адміністрації
Державної служби
спеціального зв'язку
та захисту інформації
України
24.07.2007 N 143

Зареєстровано в Міністерстві
юстиції України
8 серпня 2007 р.
за N 914/14181

ПОЛОЖЕННЯ
про порядок здійснення державного контролю
за додержанням вимог законодавства у сфері надання
послуг електронного цифрового підпису

1. Загальні положення

1.1. Це Положення розроблене відповідно до Законів України "Про електронний цифровий підпис" ([852-15](#)), "Про Державну службу спеціального зв'язку та захисту інформації України" ([3475-15](#)), Положення про Адміністрацію Державної служби спеціального зв'язку та захисту інформації, затвердженого постановою Кабінету Міністрів України від [24.06.2006](#) N 868 ([868-2006-п](#)), Порядку акредитації центру сертифікації ключів, затвердженого постановою Кабінету Міністрів України від [13.07.2004](#) N 903 ([903-2004-п](#)), Положення про центральний засвідчувальний орган, затвердженого постановою Кабінету Міністрів України від [28.10.2004](#) N 1451 ([1451-2004-п](#)), Порядку застосування електронного цифрового підпису органами державної влади, органами місцевого самоврядування, підприємствами, установами та організаціями державної форми власності, затвердженого постановою Кабінету Міністрів України від [28.10.2004](#) N 1452 ([1452-2004-п](#)).

1.2. Положення визначає порядок здійснення державного контролю за додержанням вимог законодавства у сфері надання послуг електронного цифрового підпису (далі - ЕЦП), у тому числі проведення перевірок суб'єктів правових відносин у сфері послуг ЕЦП, визначених законом, а також оформлення і розгляд результатів перевірок.

1.3. Функції контролюючого органу у сфері надання послуг електронного цифрового підпису (далі - контролюючий орган) відповідно до статті 12 Закону України "Про електронний цифровий підпис" ([852-15](#)), підпункту 33 пункту 4 Положення про Адміністрацію Державної служби спеціального зв'язку та захисту інформації, затвердженого постановою Кабінету Міністрів України від [24.06.2006](#) N 868 ([868-2006-п](#)), здійснює Адміністрація Державної служби спеціального зв'язку та захисту інформації України.

1.4. Дія Положення поширюється на контролюючий орган, центральний засвідчувальний орган, акредитовані центри сертифікації ключів (далі - акредитовані центри), центри сертифікації ключів, засвідчувальні центри органів виконавчої влади або

інших державних органів (далі - засвідчувальні центри), а також міністерства, інші центральні органи виконавчої влади, органи місцевого самоврядування (далі - державні установи).

2. Визначення термінів

2.1. Терміни, які вживаються у Положенні, мають таке значення:

безвізний нагляд - діяльність контролюючого органу, пов'язана зі збором інформації від суб'єктів правових відносин у сфері послуг ЕЦП з метою отримання відомостей про явища та процеси, що відбуваються у сфері послуг ЕЦП;

державний контроль за додержанням вимог законодавства у сфері надання послуг ЕЦП (далі - контроль у сфері ЕЦП) - це діяльність контролюючого органу в межах повноважень, передбачених законом, щодо виявлення та запобігання порушенням вимог законодавства суб'єктами правових відносин у сфері послуг ЕЦП;

перевірка - плановий або позаплановий захід контролю у сфері ЕЦП, який проводиться посадовими особами відповідно до їх функціональних повноважень за місцезнаходженням суб'єкта перевірки та здійснюється за комплексом питань або окремих питань, визначених у цьому Положенні.

Інші терміни вживаються у значеннях, визначених у Законах України "Про електронний цифровий підпис" ([852-15](#)), "Про електронні документи та електронний документообіг" ([851-15](#)), постанові Кабінету Міністрів України від [13.07.2004](#) N 903 ([903-2004-п](#)) "Про затвердження Порядку акредитації центру сертифікації ключів", наказі Департаменту спеціальних телекомунікаційних систем та захисту інформації Служби безпеки України (далі - ДСТСЗІ СБ України) від [13.01.2005](#) N 3 ([z0104-05](#)) "Про затвердження Правил посиленої сертифікації", зареєстрованому в Мін'юсті України [27.01.2005](#) за N 104/10384.

3. Контроль у сфері ЕЦП

3.1. Контроль у сфері ЕЦП реалізується контролюючим органом шляхом погодження нормативно-правових актів у випадках, передбачених законодавством та Положенням, перевірок суб'єктів правових відносин у сфері послуг ЕЦП, визначених законом, а також вжиття заходів у разі невиконання або неналежного виконання ними обов'язків, встановлених законодавством.

3.2. Основними завданнями контролю у сфері ЕЦП є:

встановлення відповідності вимогам законодавства організації та порядку надання послуг ЕЦП суб'єктами правових відносин у сфері послуг ЕЦП;

забезпечення дотримання вимог законодавства центральним засвідчувальним органом, засвідчувальними центрами щодо акредитації центрів сертифікації ключів;

своєчасне попередження, виявлення та припинення дій або бездіяльності, які містять ознаки порушення законодавства у сфері надання послуг ЕЦП, усунення причин виникнення цих порушень і умов, що їм сприяють, а в разі, якщо порушення припинено, - вжиття заходів для усунення наслідків цих порушень;

оцінка діяльності суб'єктів правових відносин у сфері послуг електронного цифрового підпису щодо дотримання законодавства;

забезпечення відповідності законодавству порядку застосування ЕЦП державними установами.

3.3. Безвізний нагляд проводиться шляхом аналізу:

стану роботи електронних інформаційних ресурсів, які використовуються для надання послуг ЕЦП;

інформаційних матеріалів, електронних документів тощо, розміщених на електронних інформаційних ресурсах, які використовуються для надання послуг ЕЦП, щодо їх відповідності вимогам законодавства;

відповідності вимогам законодавства змісту сертифікатів ключів, що формуються суб'єктами надання послуг ЕЦП;

переліку та порядку надання послуг ЕЦП через електронні інформаційні ресурси;

щорічних звітів, що надаються акредитованими центрами та центрами сертифікації ключів відповідно до пункту 3.4 Положення;

іншої інформації щодо функціонування, організації та надання послуг суб'єктами правових відносин у сфері послуг ЕЦП.

3.4. До 15 січня кожного року акредитований центр та центр сертифікації ключів надає до контролюючого органу відомості за попередній рік роботи щодо надання послуг ЕЦП, зокрема про:

кількість укладених договорів про надання послуг ЕЦП (окремо з фізичними та юридичними особами);

кількість сформованих та скасованих сертифікатів ключів за звітний період із зазначенням причин скасування;

факти відшкодування збитків підписувачам, користувачам або третім особам внаслідок неналежного виконання акредитованим центром та центром сертифікації ключів своїх зобов'язань (за наявністю);

факти участі як позивача, відповідача або третьої сторони у судових справах з питань, пов'язаних з наданням послуг ЕЦП, предмет розгляду та прийняте рішення (за наявністю);

факти порушень акредитованим центром та центром сертифікації ключів вимог законодавства із захисту інформації під час надання послуг ЕЦП, їх причини та заходи щодо усунення порушень;

інші питання за окремими запитами контролюючого органу.

3.5. Контролюючим органом організуються та проводяться планові та позапланові перевірки суб'єктів правових відносин у сфері послуг ЕЦП, визначених законом.

3.6. Предметом перевірки центрального засвідчувального органу, засвідчувальних центрів та акредитованих центрів є стан дотримання законодавства у сфері надання послуг ЕЦП, у тому числі Закону України "Про електронний цифровий підпис" ([852-15](#)), постанови Кабінету Міністрів України від [13.07.2004](#) N 903 ([903-2004-п](#)) "Про затвердження Порядку акредитації центру сертифікації ключів", постанови Кабінету Міністрів України від [28.10.2004](#) N 1451 ([1451-2004-п](#)) "Про затвердження Положення про центральний засвідчувальний орган", наказу ДСТСЗІ СБ України від [13.01.2005](#) N 3 ([z0104-05](#)) "Про затвердження Правил посиленої сертифікації", зареєстрованого в Мін'юсті України [27.01.2005](#) за N 104/10384, інших нормативно-правових актів, а також регламенту роботи акредитованого центру.

3.7. Під час перевірки акредитованого центру можуть перевірятися його відокремлені пункти реєстрації.

3.8. Предметом перевірки центрів сертифікації ключів є стан дотримання положень Закону України "Про електронний цифровий підпис" під час надання послуг ЕЦП.

3.9. Контроль за діяльністю державних установ щодо дотримання вимог законодавства у сфері ЕЦП здійснюється шляхом погодження проектів нормативно-правових актів, що визначають порядок застосування ЕЦП державною установою.

Перевірки державних установ стосовно дотримання вимог законодавства із захисту інформації, яка є власністю держави, або інформації з обмеженим доступом, вимога щодо захисту якої встановлена законом, у тому числі під час застосування ЕЦП, здійснюються Державною службою спеціального зв'язку та захисту інформації України (далі - Держспецзв'язку) в рамках державного контролю за станом криптографічного захисту інформації.

3.10. У разі виявлення фактів (ознак) порушення вимог законодавства у сфері ЕЦП контролюючий орган має право звернутися до державної установи щодо припинення дій або усунення порушень законодавства та вимагати звіту про здійснення заходів із усунення порушень.

4. Організація проведення перевірок

4.1. Планові перевірки центрального засвідчувального органу, у тому числі державного підприємства, установи та організації, що здійснює технічне та технологічне забезпечення виконання функцій центрального засвідчувального органу відповідно до пункту 7 Положення про центральний засвідчувальний орган, затвердженого постановою Кабінету Міністрів України від 28.10.2004 N 1451 ([1451-2004-п](#)), а також інших суб'єктів у сфері послуг ЕЦП, встановлених законом, проводиться відповідно до плану перевірок, який складається на кожний рік та затверджується Адміністрацією Держспецзв'язку до 1 грудня року, що передує плановому. Копія плану перевірок направляється до центрального засвідчувального органу протягом 10 робочих днів з дня його затвердження.

4.2. Періодичність проведення планових перевірок встановлюються законодавством з урахуванням ступеня ризику від здійснення діяльності, пов'язаної з наданням послуг ЕЦП.

4.3. Щорічно до 1 квітня контролюючий орган готує звіт про виконання річного плану перевірок за попередній рік і оприлюднює його в мережі Інтернет.

4.4. Позапланова перевірка суб'єктів у сфері послуг ЕЦП здійснюється за рішенням контролюючого органу за наявності таких підстав:

подання суб'єктом у сфері послуг ЕЦП письмової заяви до контролюючого органу про здійснення перевірки за його бажанням;

виявлення та підтвердження недостовірності даних, заявлених у щорічних звітах, що надаються акредитованими центрами та центрами сертифікації ключів відповідно до пункту 3.4 Положення (для акредитованих центрів та центрів сертифікації ключів);

перевірка виконання суб'єктом у сфері послуг електронного цифрового підпису приписів щодо усунення порушень вимог законодавства, виданих за результатами проведення планової перевірки;

подання пропозицій центральним засвідчувальним органом контролюючому органу за результатами розгляду заяв і скарг щодо неналежного функціонування акредитованих центрів або центрів сертифікації ключів (для акредитованих центрів та центрів сертифікації ключів);

письмового повідомлення центральним засвідчувальним органом про обставини, які перешкоджають його діяльності (для центрального засвідчувального органу);

письмового звернення підписувачів та користувачів щодо неналежного виконання суб'єктами у сфері послуг ЕЦП функцій, визначених законодавством;

неподання у встановлений термін акредитованими центрами та центрами сертифікації ключів щорічних звітів відповідно до пункту 3.4 Положення без поважних

причин, а також письмових пояснень про причини, які перешкоджали поданню таких звітів (для акредитованих центрів та центрів сертифікації ключів);
звернення суду.

4.5. Під час проведення позапланової перевірки з'ясовуються лише ті питання, необхідність перевірки яких стала підставою для здійснення цього заходу, з обов'язковим зазначенням цих питань у посвідченні на проведення перевірки.

4.6. Суб'єкт перевірки повинен ознайомитися з підставою проведення позапланової перевірки з наданням йому копії відповідного документа.

4.7. Строк здійснення позапланової перевірки не може перевищувати десяти робочих днів. Продовження строку здійснення позапланової перевірки не допускається.

4.8. Про проведення планової перевірки контролюючий орган письмово повідомляє відповідного суб'єкта не пізніше ніж за 10 днів до початку цієї перевірки.

Повідомлення повинно містити:

дату початку та дату закінчення здійснення перевірки;

найменування суб'єкта перевірки;

найменування контролюючого органу.

Повідомлення надсилається рекомендованим листом чи телефонограмою або вручається особисто керівнику чи уповноваженій особі суб'єкта перевірки під розписку.

4.9. Суб'єкт перевірки має право не допускати посадових осіб контролюючого органу до здійснення планової перевірки в разі неодержання повідомлення про здійснення перевірки.

4.10. Для проведення перевірки контролюючий орган видає наказ, який має містити найменування суб'єкта перевірки, предмет перевірки та склад комісії з перевірки (далі - Комісія).

4.11. До складу Комісії можуть залучатися в установленому порядку представники центрального засвідчувального органу.

4.12. На підставі наказу оформляється посвідчення на проведення перевірки, яке підписується Головою Держспецзв'язку або його заступником і засвідчується печаткою.

У посвідченні на проведення перевірки зазначаються:

найменування контролюючого органу;

найменування суб'єкта перевірки;

місцезнаходження суб'єкта перевірки;

номер і дата наказу, на виконання якого здійснюється перевірка;

склад Комісії із зазначенням посад, прізвищ, імен та по батькові її членів;

дата початку та дата закінчення перевірки;

тип перевірки (планова або позапланова);

підстави перевірки;

перелік питань, що підлягають перевірці;

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

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

4.13. Строк здійснення планової перевірки не може перевищувати п'ятнадцяти робочих днів. Продовження строку здійснення перевірки не допускається.

5. Права та обов'язки Комісії

5.1. Голова Комісії зобов'язаний:
забезпечити координацію роботи між членами Комісії при підготовці та проведенні перевірки;
організувати роботу Комісії, у тому числі визначити конкретні терміни, види, обсяги робіт, що потрібні для проведення перевірки;
здійснити розподіл питань, за якими проводиться перевірка, між членами Комісії, встановити порядок і режим їх роботи;
контролювати виконання доручених ним завдань.

5.2. Голова Комісії має право:
встановлювати для членів Комісії додаткові завдання з перевірки та здійснювати перерозподіл їх обов'язків;
здійснювати особисто перевірку будь-якої діяльності суб'єкта перевірки у сфері надання послуг ЕЦП;
запитувати та отримувати від підписувачів, яким надаються послуги ЕЦП суб'єктом перевірки, за їх згодою, відомості, що потрібні для встановлення фактичних обставин, які призвели (можуть призвести) до порушень встановлених вимог стосовно надання послуг ЕЦП;
давати вказівки щодо оформлення акта перевірки та припису;
давати інші вказівки щодо проведення перевірки.

5.3. Члени Комісії беруть участь у роботі Комісії та виконують поставлені перед ними завдання. Член Комісії має право одноособово, керуючись конкретним завданням голови Комісії, досліджувати окремі питання перевірки.

5.4. Члени Комісії зобов'язані:
повно, об'єктивно та неупереджено здійснювати перевірку;
керуватися та дотримуватися вимог законодавства та нормативно-правових актів з питань надання послуг ЕЦП і захисту інформації;
сумлінно, вчасно та якісно виконувати свої службові обов'язки та доручення голови Комісії;
дотримуватися ділової етики у взаємовідносинах із суб'єктами перевірки;
ознайомити керівника суб'єкта перевірки або його заступника, або уповноважену ним особу з результатами перевірки;
надавати суб'єкту перевірки консультаційну допомогу щодо здійснення перевірки;
не розголошувати інформацію з обмеженим доступом, яка стала їм відома в зв'язку з виконанням службових обов'язків.

5.5. Члени Комісії при виконанні своїх службових обов'язків під час проведення перевірки мають право:
вільного доступу встановленим порядком до всіх документів та інформації суб'єкта перевірки щодо надання ним послуг ЕЦП і акредитації, у тому числі інформації з обмеженим доступом;
вільного доступу у робочий час на територію та до всіх приміщень суб'єкта перевірки, у тому числі спеціальних, які використовуються для забезпечення функціонування технічних засобів та зберігання документів з питань надання послуг ЕЦП;

вивчати роботу технічних засобів, які використовуються суб'єктом перевірки для надання послуг у сфері ЕЦП, у тому числі автоматизованих систем та програмно-технічного комплексу;

одержувати від посадових осіб інформацію та пояснення (у тому числі за рішенням голови Комісії - письмові) щодо їх діяльності з питань надання послуг ЕЦП (акредитації), необхідні для здійснення перевірки;

отримувати від суб'єкта перевірки та долучати до матеріалів перевірки копії документів, у тому числі виготовлені методом сканування або створення фотокопій, що можуть свідчити про факти порушення суб'єктом перевірки законодавства у сфері надання послуг ЕЦП;

пред'являти до керівників і працівників суб'єкта перевірки інші вимоги, що пов'язані з їх обов'язками, передбаченими Положенням.

5.6. Голова та члени Комісії несуть відповідальність згідно з законодавством за: необ'єктивне відображення у акті перевірки даних щодо діяльності суб'єкта перевірки;

приховування фактів порушень чи зловживань, виявлених під час перевірки; інші дії, вчинені в процесі перевірки, які порушують законодавство.

6. Порядок проведення перевірки

6.1. Перевірка складається з таких етапів:
підготовка до проведення перевірки;
процес перевірки;
оформлення результатів перевірки.

6.2. Підготовка до проведення перевірки здійснюється шляхом:
опрацювання матеріалів попередньої перевірки з метою подальшого контролю за тими напрямками роботи, за якими раніше були виявлені порушення;
аналізу матеріалів безвиїзного нагляду;
вивчення регламенту роботи суб'єкта перевірки.

6.3. Контролюючий орган має право письмово запитувати у суб'єктів у сфері послуг ЕЦП матеріали та інформацію, необхідні для проведення перевірки. Суб'єкти у сфері послуг ЕЦП зобов'язані надати контролюючому органу всю потрібну інформацію протягом п'ятнадцяти робочих днів після отримання відповідного запиту.

6.4. У період підготовки до проведення перевірки голова Комісії інформує її членів про завдання (рекомендації, вказівки) перевірки, а також проводить інструктаж щодо порядку взаємодії з працівниками суб'єкта перевірки.

6.5. Перед початком здійснення перевірки члени Комісії зобов'язані пред'явити керівнику суб'єкта перевірки або уповноваженій ним особі посвідчення та службові посвідчення, що засвідчують посадових осіб контролюючого органу, і надати суб'єкту перевірки копію посвідчення на проведення перевірки.

6.6. Посадові особи контролюючого органу без посвідчення на здійснення перевірки та службових посвідчень не мають права здійснювати перевірку.

6.7. Керівники суб'єкта перевірки зобов'язані створити необхідні умови для проведення перевірки, а саме:

забезпечити на період проведення перевірки кожному члену Комісії безперешкодний вхід до/вихід із усіх приміщень суб'єкта перевірки протягом усього робочого дня за умови дотримання порядку здійснення перевірки, передбаченого законодавством;

надати членам Комісії у день початку перевірки службове приміщення, яке обладнане потрібними меблями, комп'ютером та сховищем для документів. На весь період перевірки вхід до зазначеного приміщення особам, що не є членами Комісії, які здійснюють перевірку, без дозволу голови Комісії забороняється.

Якщо немає можливості виділити Комісії ізольоване від працівників суб'єкта перевірки службове приміщення, то, за згодою її голови, керівники суб'єкта перевірки повинні надати членам Комісії окреме робоче місце, обладнане таким чином, щоб забезпечити належні умови для роботи Комісії;

організувати зустріч членів Комісії з керівниками відповідних служб, що підлягають перевірці;

забезпечити членам Комісії вільний доступ до всіх документів та інформації про діяльність суб'єкта перевірки з питань надання послуг ЕЦП;

забезпечити надання в установлені членами Комісії терміни документів та інформації про діяльність суб'єкта перевірки, пояснень (письмово й усно);

на вимогу голови Комісії забезпечити надання копій документів, їх реєстрацію встановленим порядком;

засвідчувати надані пояснення щодо отриманої інформації, документів;

забезпечувати коректну поведінку своїх підлеглих під час проведення перевірки.

6.8. Керівники суб'єкта перевірки мають право:

вимагати від посадових осіб контролюючого органу додержання вимог законодавства;

перевіряти наявність у посадових осіб контролюючого органу службових посвідчень і одержувати копії посвідчення на проведення планової або позапланової перевірки;

не допускати посадових осіб контролюючого органу до здійснення перевірки, якщо:

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

- посадова особа контролюючого органу не надала копії документів, передбачених Положенням, або якщо надані документи не відповідають вимогам Положення;

бути присутнім під час здійснення перевірки;

вимагати нерозголошення інформації, що є комерційною таємницею суб'єкта перевірки;

одержувати та ознайомлюватися з актами за результатами перевірки;

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

отримувати від голови Комісії роз'яснення щодо дій Комісії, пов'язаних з перевіркою;

у разі неузгодження з діями голови та/або членів Комісії подавати в письмовому вигляді скарги до керівництва контролюючого органу чи оскаржувати дії Комісії в судовому порядку.

6.9. Перед початком перевірки голова Комісії вносить запис до відповідного журналу суб'єкта перевірки (за його наявності).

6.10. Перевірка здійснюється у присутності керівника суб'єкта перевірки або його заступника, або вповноваженої особи суб'єкта перевірки.

6.11. Перевірка центрального засвідчувального органу, засвідчувального центру проводиться за Переліком питань, які підлягають перевірці в центральному засвідчувальному органі та засвідчувальному центрі (додаток 1). Перевірка акредитованого центру проводиться за Переліком питань, які підлягають перевірці в акредитованому центрі (додаток 2). Перевірка центру сертифікації ключів проводиться з питань виконання обов'язків, визначених статтею 8 Закону України "Про електронний цифровий підпис" (852-15).

6.12. Перевірка проводиться шляхом вивчення документів, інформації, що міститься в базах даних, співбесід з працівниками суб'єкта перевірки, аналізу стану виконання вимог нормативно-правових актів та внутрішніх розпорядчих документів з питань надання послуг ЕЦП.

6.13. Перевірки організуються таким чином, щоб не порушувати режим роботи суб'єкта перевірки.

6.14. У міру виявлення порушень законодавства, зловживань і недоліків керівництву суб'єкта перевірки, не чекаючи закінчення перевірки, слід уживати заходів щодо усунення виявлених порушень, зловживань і недоліків, запобігання їм надалі.

7. Порядок оформлення результатів перевірки

7.1. За результатами перевірки члени Комісії складають акт перевірки. Акт перевірки складається у довільній формі та містить такі відомості:

- дату складання акта;
- тип перевірки (планова або позапланова);
- предмет державного контролю;
- найменування контролюючого органу, а також посади, прізвища, ініціали голови та членів Комісії;
- найменування суб'єкта перевірки;
- прізвище та ініціали керівника суб'єкта перевірки;
- місце проведення перевірки (місцезнаходження суб'єкта перевірки);
- термін проведення перевірки;
- дату та номер посвідчення на перевірку;
- період, за який проводилася перевірка;
- опис організаційної структури суб'єкта перевірки;
- результати попередньої перевірки;
- назву та короткий зміст документів, наданих під час перевірки;
- що було встановлено під час перевірки, у тому числі висвітлити показники, які характеризують роботу суб'єкта перевірки в цілому;
- виявлені під час перевірки порушення і недоліки, їх вплив на стан надання послуг у сфері ЕЦП;
- висновки за результатами перевірки;
- факти протидії проведенню перевірки (якщо такі були);
- підписи голови та членів Комісії;
- підпис керівника суб'єкта перевірки або особи, що його замінює, про ознайомлення з актом перевірки.

7.2. 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

пункти, статті, розділи нормативно-правових актів, що порушені. Довільне трактування нормативно-правових актів не допускається.

Довідкову або однорідну інформацію про порушення і недоліки, яка може бути згрупована, 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.

7.3. Акт перевірки складається у двох примірниках та підписується не пізніше останнього дня перевірки всіма членами Комісії та керівником суб'єкта перевірки або особою, що його замінює.

7.4. Член Комісії, який не погоджується з висновками Комісії, 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".

7.5. Якщо керівник суб'єкта перевірки має зауваження щодо фактів та висновків, викладених в акті перевірки, то перед підписом робить запис "Із зауваженнями, що додаються". Зауваження оформлюються окремим документом та засвідчуються підписом керівника суб'єкта перевірки. Зауваження керівника суб'єкта перевірки та окрема думка члена Комісії є невід'ємною частиною акта перевірки.

7.6. Якщо керівник суб'єкта перевірки відмовився від ознайомлення з актом перевірки або від його підписання після ознайомлення з ним, голова Комісії перед місцем для підпису керівника суб'єкта перевірки робить відповідну відмітку, яка завіряється підписами голови та одного з членів Комісії.

7.7. Один примірник акта перевірки залишається в контролюючому органі, другий - у строк не більше п'яти робочих днів після завершення перевірки вручається представнику суб'єкта перевірки або надсилається рекомендованим листом з підтвердженням поштового відправлення. У разі перевірки акредитованого центру, копія акта протягом п'яти робочих днів після завершення перевірки направляється до центрального засвідчувального органу.

8. Порядок розгляду результатів перевірки

8.1. На підставі акта, який складено за результатами здійснення перевірки, у ході якої виявлено порушення вимог законодавства, протягом п'яти робочих днів з дня завершення перевірки складається припис про усунення порушень, виявлених під час перевірки. Припис видається та підписується членами Комісії, які здійснювали перевірку.

8.2. Припис щодо усунення порушень складається у двох примірниках: один примірник не пізніше п'яти робочих днів з дня складання акта надається суб'єкту перевірки чи вповноваженій ним особі для виконання, а другий примірник з підписом суб'єкта перевірки або вповноваженої ним особи щодо погоджених термінів усунення порушень вимог законодавства залишається в контролюючому органі.

8.3. У разі відмови суб'єкта перевірки або вповноваженої ним особи від отримання припису щодо усунення порушень вимог законодавства він направляється рекомендованим листом, а на копії припису, який залишається в контролюючому органі, проставляються відповідний вихідний номер і дата направлення.

8.4. Керівник суб'єкта перевірки повинен ужити заходів щодо усунення недоліків та порушень, зазначених у приписі, протягом визначеного терміну.

8.5. Суб'єкт перевірки зобов'язаний у встановлений в приписі термін письмово подати контролюючому органу інформацію про усунення порушень разом з документами, що це підтверджують.

8.6. У разі встановлення за результатами проведеної перевірки акредитованого центру та центру сертифікації ключів фактів (ознак) компрометації особистого ключа порушення вимог законодавства у сфері послуг ЕЦП, не усунених за встановлений у приписі термін, недостовірних даних, зазначених у сертифікаті ключа, контролюючим органом розглядаються надані матеріали та відповідно до статті 12 Закону України "Про електронний цифровий підпис" ([852-15](#)) вирішуються питання щодо видання розпорядження центральному засвідчувальному органу про застосування заходів стосовно суб'єкта перевірки (далі - розпорядження центральному засвідчувальному органу) відповідно до закону.

8.7. Розпорядження центральному засвідчувальному органу може містити вимогу про скасування сертифіката ключа акредитованого центру або центру сертифікації ключів.

8.8. Розпорядження центральному засвідчувальному органу обов'язково повинно містити:

дату складання;

найменування контролюючого органу, а також посади, прізвища, ім'я та по-батькові членів Комісії, які здійснили перевірку;

найменування та місцезнаходження суб'єкта перевірки, а також прізвище, ім'я та по батькові його керівника чи вповноваженої ним особи, щодо діяльності якого здійснювалася перевірка;

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

обґрунтовані підстави видання розпорядження центральному засвідчувальному органу;

вимогу щодо застосування заходів стосовно суб'єкта перевірки.

8.9. На підставі розпорядження центральному засвідчувальному органу він уживає заходів стосовно суб'єкта перевірки, що передбачені законом.

**Начальник Департаменту
регулювання діяльності
у сфері криптографічного
захисту інформації
Адміністрації Держспецзв'язку**

В.П.Гребнів

Додаток 1
до пункту 6.11
Положення про порядок
здійснення державного контролю
за додержанням вимог
законодавства у сфері надання
послуг електронного цифрового
підпису

ПЕРЕЛІК
питань, які підлягають перевірці
в центральному засвідчувальному органі
та засвідчувальному центрі

1. Організаційні питання

1.1. Відповідність спеціального приміщення встановленим вимогам, організація охорони спеціального приміщення та порядок доступу у спеціальне приміщення.

1.2. Наявність чинного експертного висновку на програмно-технічний комплекс, виданого за результатами державної експертизи у сфері криптографічного захисту інформації.

1.3. Наявність атестата відповідності комплексної системи захисту інформації вимогам нормативних документів з питань захисту інформації, відповідність складу програмних та технічних засобів, зазначених в експертному висновку до атестата відповідності комплексної системи захисту інформації.

1.4. Наявність погодженого з контролюючим органом регламенту роботи.

1.5. Наявність штатних або найманих за договором спеціалістів, призначених на посади адміністратора безпеки, адміністратора сертифікації, адміністратора реєстрації, системного адміністратора, наявність положення, яким визначаються посадові обов'язки, кваліфікаційні вимоги та відповідальність посадових осіб, діяльність яких безпосередньо пов'язана з наданням послуг ЕЦП та обслуговуванням сертифікатів ключів. Знання посадових обов'язків особами, діяльність яких безпосередньо пов'язана з наданням послуг ЕЦП та обслуговуванням сертифікатів ключів.

1.6. Наявність нормативних документів, що визначають порядок забезпечення безпеки експлуатації програмно-технічного комплексу, порядок генерації ключових даних та поводження з ключовими документами. Наявність служби захисту інформації, а також положення про службу захисту інформації.

1.7. Узяття на облік програмно-технічного комплексу та інших засобів криптографічного захисту інформації, що використовуються.

1.8. Порядок зберігання резервних копій сертифікатів та списків відкликаних сертифікатів.

1.9. Дотримання вимог із захисту інформації, яка обробляється в автоматизованих системах центрального засвідчувального органу (засвідчувального центру).

2. Технічні та технологічні питання

2.1. Ведення журналів аудиту щодо подій, пов'язаних з генерацією, використанням та знищенням особистого ключа.

2.2. Розміщення, зберігання, доступ та використання особистого ключа.

2.3. Розміщення, зберігання та доступ до резервної копії особистого ключа.

2.4. Порядок реєстрації (формування сертифіката ключа) центру сертифікації ключів. Відповідність порядку реєстрації політиці сертифікації та регламенту роботи.

2.5. Зберігання сформованих сертифікатів ключів, а також сертифікатів та документованої інформації, яка підлягає обов'язковій передачі центрами сертифікації ключів у разі припинення їх діяльності.

2.6. Відповідність змісту сформованих сертифікатів установленим законодавством вимогам.

2.7. Розміщення на електронному інформаційному ресурсі документів та інформації, установлених політикою сертифікації.

2.8. Ведення журналів аудиту щодо подій, пов'язаних з формуванням, скасуванням, блокуванням та поновленням сертифікатів ключів.

2.9. Функціонування електронного інформаційного ресурсу щодо надання доступу до основних даних (реквізитів) акредитованих центрів, центрів сертифікації ключів, переліку сертифікатів центрів сертифікації ключів, а також інформації про статус сертифікатів.

2.10. Ведення журналів аудиту програмно-технічного комплексу.

3. Питання, пов'язані з акредитацією центрів сертифікації ключів

3.1. Відомості, що подають центри сертифікації ключів для акредитації.

3.2. Програми, методики та результати (протоколи) досліджень щодо відповідності центру сертифікації ключів установленим вимогам для акредитованого центру сертифікації ключів.

3.3. Ведення Реєстру суб'єктів, які надають послуги, пов'язані з електронним цифровим підписом.

3.4. Результати розгляду заяв та скарг щодо неналежного функціонування центрів сертифікації ключів.

Начальник Департаменту
регулювання діяльності
у сфері криптографічного
захисту інформації
Адміністрації Держспецзв'язку

В.П.Гребнев

Додаток 2
до пункту 6.11
Положення про порядок
здійснення державного
контролю за додержанням
вимог законодавства у сфері
надання послуг електронного
цифрового підпису

ПЕРЕЛІК
питань, які підлягають перевірці
в акредитованому центрі

1. Організаційні питання

1.1. Достовірність відомостей, наведених у документах, поданих центром сертифікації ключів для акредитації, відповідність відомостей, які зазначені у свідоцтві про акредитацію.

1.2. Наявність спеціального рахунку для забезпечення відшкодування збитків, які можуть бути завдані внаслідок неналежного виконання акредитованим центром своїх зобов'язань.

1.3. Відповідність спеціального приміщення встановленим вимогам, організація охорони спеціального приміщення та порядок доступу в спеціальне приміщення.

1.4. Наявність чинного експертного висновку на програмно-технічний комплекс, виданого за результатами державної експертизи у сфері криптографічного захисту інформації.

1.5. Наявність атестата відповідності комплексної системи захисту інформації вимогам нормативних документів з питань захисту інформації, відповідність складу програмних та технічних засобів, зазначених в експертному висновку до атестата відповідності комплексної системи захисту інформації.

1.6. Наявність погодженого з контролюючим органом регламенту роботи.

1.7. Наявність штатних або найманих за договором спеціалістів, призначених на посади адміністратора безпеки, адміністратора сертифікації, адміністратора реєстрації, системного адміністратора, наявність положення, яким визначаються посадові обов'язки, кваліфікаційні вимоги та відповідальність посадових осіб, діяльність яких безпосередньо пов'язана з наданням послуг ЕЦП та обслуговуванням сертифікатів ключів. Знання посадових обов'язків особами, діяльність яких безпосередньо пов'язана з обслуговуванням сертифікатів ключів.

1.8. Наявність нормативних документів, що визначають порядок забезпечення безпеки експлуатації програмно-технічного комплексу, порядок генерації ключових даних та поводження з ключовими документами. Наявність служби захисту інформації, а також положення про службу захисту інформації.

1.9. Узяття на облік програмно-технічного комплексу та інших засобів криптографічного захисту інформації, що використовуються.

1.10. Відповідність положень типового договору про надання послуг ЕЦП вимогам, визначеним у політиці сертифікації.

1.11. Ведення обліку укладених договорів про надання послуг ЕЦП, а також документів або їх копій, які надаються під час реєстрації підписувачів. Забезпечення захисту персональних даних користувачів.

1.12. Порядок зберігання резервних копій сертифікатів та списків відкликаних сертифікатів.

1.13. Порядок синхронізації із Всесвітнім координованим часом (UTC).

1.14. Дотримання вимог із захисту інформації, яка обробляється в автоматизованих системах акредитованого центру.

2. Технічні та технологічні питання, пов'язані з обслуговуванням сертифікатів ключів

2.1. Ведення журналів аудиту щодо подій, пов'язаних з генерацією, використанням та знищенням особистого ключа.

2.2. Розміщення, зберігання, доступ та використання особистого ключа.

2.3. Розміщення, зберігання та доступ до резервної копії особистого ключа.

2.4. Надання допомоги з генерації особистих ключів підписувачам.

2.5. Порядок реєстрації підписувачів (юридичних та фізичних осіб). Відповідність порядку реєстрації підписувачів політики сертифікації та регламенту роботи. Робота відокремлених пунктів реєстрації (у разі наявності) щодо реєстрації підписувачів.

2.6. Зберігання сформованих сертифікатів ключів.

2.7. Відповідність змісту сформованих сертифікатів установленим законодавством вимогам, зокрема щодо використання ідентифікатора політики сертифікації у сертифікатах та обов'язкових реквізитів розпізнавального імені підписувача.

2.8. Розміщення на електронному інформаційному ресурсі документів та інформації, установлених політикою сертифікації.

2.9. Управління статусом сертифікатів. Відповідність порядку блокування, поновлення та скасування сертифікатів ключів політиці сертифікації та регламенту роботи.

2.10. Ведення журналів аудиту щодо подій, пов'язаних з формуванням, скасуванням, блокуванням та поновленням сертифікатів ключів.

2.11. Функціонування електронного інформаційного ресурсу щодо надання доступу до сертифікатів акредитованого центру, інших сертифікатів, що сформовані акредитованим центром, а також інформації про статус сертифікатів.

2.12. Надання інших послуг ЕЦП, передбачених регламентом роботи.

2.13. Ведення журналів аудиту програмно-технічного комплексу.

Начальник Департаменту
регулювання діяльності
у сфері криптографічного
захисту інформації
Адміністрації Держспецзв'язку

В.П.Гребнев