Держлата регуляторна служба

Прим. № 1

ДЕРЖАВНА СЛУЖБА СПЕЦІАЛЬНОГО ЗВ'ЯЗКУ ТА ЗАХИСТУ ІНФОРМАЦІЇ УКРАЇНИ

вул. Солом'янська, 13, м. Київ, 03110,
тел. (044) 281-92-10, факс: (044) 281-94-83, e-mail: info@dsszzi.gov.ua

18.09.18 № 04/02/03-2901

Державні органи
(згідно зі списком на розсилку)

Про погодження проекту наказу
Адміністрації Держспецзв'язку

Надсилаємо на погодження проект наказу Адміністрації Державної служби спеціального зв'язку та захисту інформації України «Про встановлення вимог з безпеки та захисту інформації до кваліфікованих надавачів електронних довірчих послуг та їхніх відокремлених пунктів реєстрації», підготовленого на виконання абзацу третього частини другої статті 8, абзацу третього частини другої статті 13, абзацу третього пункту 8 розділу VII «Прикінцеві та перехідні положення» Закону України «Про електронні довірчі послуги».

Просимо розглянути та погодити проект наказу у строк до 20.09.2018.

Додатки: 1. Проект наказу на 10 арк.
2. Пояснювальна записка до проекту наказу на 6 арк.
3. Аналіз регуляторного впливу проекту наказу на 17 арк., тільки на першу адресу.
4. Повідомлення про оприлюднення на 4 арк., тільки на першу адресу.

Голова Служби Л.О. Євдоченко

Вик. Гавриков А.В.
Тел. 281-94-91

Державна регуляторна служба України
№ 13031/0/19-18 від 24.09.2018

0.31

ПРОЕКТ

АДМІНІСТРАЦІЯ ДЕРЖАВНОЇ СЛУЖБИ СПЕЦІАЛЬНОГО ЗВ'ЯЗКУ ТА ЗАХИСТУ ІНФОРМАЦІЇ УКРАЇНИ

Н А К А З

м. Київ

___.___.2018 № ____

Про встановлення вимог з безпеки та захисту інформації до кваліфікованих надавачів електронних довірчих послуг та їхніх відокремлених пунктів реєстрації

Відповідно до абзацу третього частини другої статті 8 Закону України «Про електронні довірчі послуги», пункту 37 частини першої статті 14 Закону України «Про Державну службу спеціального зв'язку та захисту інформації України» та підпункту 2 пункту 3 Положення про Адміністрацію Державної служби спеціального зв'язку та захисту інформації України, затвердженого постановою Кабінету Міністрів України від 3 вересня 2014 року № 411, та з метою удосконалення законодавства у сфері електронних довірчих послуг

НАКАЗУЮ:

1. Затвердити вимоги з безпеки та захисту інформації до кваліфікованих надавачів електронних довірчих послуг та їхніх відокремлених пунктів реєстрації, що додаються.

2. Визнати такими, що втратили чинність:

1) наказ Департаменту спеціальних телекомунікаційних систем та захисту інформації Служби безпеки України від 13 січня 2005 року № 3 «Про затвердження Правил посиленої сертифікації», зареєстрований в Міністерстві юстиції України 27 січня 2005 року за № 104/10384;

2) наказ Департаменту спеціальних телекомунікаційних систем та захисту інформації Служби безпеки України від 10 травня 2006 року № 50 «Про внесення змін до Правил посиленої сертифікації», зареєстрований в Міністерстві юстиції України 17 травня 2006 року за № 568/12442;

3) наказ Адміністрації Державної служби спеціального зв'язку та захисту інформації України від 24 липня 2007 року № 143 «Про затвердження Положення про порядок здійснення державного контролю за додержанням вимог законодавства у сфері електронного цифрового підпису», зареєстрований в Міністерстві юстиції України 8 серпня 2007 року за № 914/14181;

4) пункт 4 Змін до нормативно-правових актів Адміністрації Держспецзв'язку з питань доступу до інформації, затверджених наказом Адміністрації Державної служби спеціального зв'язку та захисту інформації України від 2 березня 2012 року № 90, зареєстрований в Міністерстві юстиції України 21 березня 2012 року за № 421/20734;

5) наказ Адміністрації Державної служби спеціального зв'язку та захисту інформації України від 16 вересня 2014 року № 462 «Про внесення змін до наказу Адміністрації Держспецзв'язку від 24 липня 2007 року № 143», зареєстрований в Міністерстві юстиції України 8 жовтня 2014 року за № 1217/25994;

6) наказ Адміністрації Державної служби спеціального зв'язку та захисту інформації України від 10 червня 2016 року № 381 «Про затвердження Змін до Положення про порядок здійснення державного контролю за додержанням вимог законодавства у сфері електронного цифрового підпису, затвердженого наказом Адміністрації Державної служби

спеціального зв'язку та захисту інформації України від 24 липня 2007 року № 143», зареєстрований в Міністерстві юстиції України 5липня 2016 року за № 926/29056.

3. Директору Департаменту захисту інформації Адміністрації Державної служби спеціального зв'язку та захисту інформації України у п'ятиденний строк після підписання цього наказу в установленому порядку забезпечити його подання на державну реєстрацію до Міністерства юстиції України.

4. Цей наказ набирає чинності з 07 листопада 2018 року.

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

Голова Служби Л.О. Євдоченко

ЗАТВЕРДЖЕНО

Наказ Адміністрації Державної служби спеціального зв'язку та захисту інформації України _____ 2018 року № ___

Вимоги

з безпеки та захисту інформації до кваліфікованих надавачів електронних довірчих послуг та їхніх відокремлених пунктів реєстрації

I. Загальні положення

1. Положення цих Вимог є обов'язковими для кваліфікованих надавачів електронних довірчих послуг (далі – надавач) під час надання ними кваліфікованих електронних довірчих послуг (далі – послуги) користувачам електронних довірчих послуг (далі – користувач) та відокремлених пунктів реєстрації (далі – ВПР) під час реєстрації підписувачів в частині, що стосується.

2. Безпека інформаційних ресурсів надавача та ВПР досягається шляхом впровадження системи управління інформаційної безпеки (далі – СУІБ) та комплексної системи захисту інформації (далі – КСЗІ) інформаційно-телекомунікаційної системи (далі – ІТС) з підтвердженою відповідністю.

3. Відповідність КСЗІ ІТС вимогам законодавства у сфері захисту інформації підтверджується атестатом відповідності та позитивним

експертним висновком за результатами державної експертизи в сфері технічного захисту інформації.

Підтвердження відповідності КСЗІ ІТС надавача здійснюється у порядку, визначеному Адміністрацією Державної служби спеціального зв'язку та захисту інформації України.

Відповідність СУІБ надавача вимогам законодавства у сфері управління інформаційною безпекою підтверджується документом про відповідність, складеного за результатами проведення процедури оцінки відповідності відповідно до вимог законодавства у сфері оцінки відповідності.

4. Надання кваліфікованих електронних довірчих послуг надавачем без чинних документів, що підтверджують відповідність КСЗІ ІТС надавача та засобів захисту інформації у її складі вимогам законодавства у сфері захисту інформації, та СУІБ надавача вимогам законодавства у сфері управління інформаційною безпекою забороняється.

5. Ці Вимоги базуються на нормах національних стандартів України:

ДСТУ ETSI EN 319 401:2016 «Електронні підписи й інфраструктури (ESI). Загальні вимоги політики для провайдерів довірчих послуг», затвердженого наказом державного підприємства «Український науково-дослідний і навчальний центр проблем стандартизації, сертифікації та якості» від 21 червня 2016 року № 183, (ETSI EN 319 401:2016, IDT) (далі – ДСТУ ETSI EN 319 401);

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

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

ДСТУ ETSI EN 319 421:2016 «Електронні підписи й інфраструктури (ESI). Політика та вимоги безпеки щодо провайдерів трастових послуг, які видають часові штемпелі», затвердженого наказом державного підприємства «Український науково-дослідний і навчальний центр проблем стандартизації, сертифікації та якості» від 21 червня 2016 року № 183, (ETSI EN 319 421:2016, IDT) (далі – ДСТУ ETSI EN 319 421);

ДСТУ ISO/IEC 27001:2015 «Інформаційні технології. Методи захисту. Системи управління інформаційною безпекою. Вимоги», затверджений наказом державного підприємства «Український науково-дослідний і навчальний центр проблем стандартизації, сертифікації та якості» від 18 грудня 2015 року № 193, (ISO/IEC 27001:2013; Cor 1:2014, IDT) (далі – ДСТУ ISO/IEC 27001);

ДСТУ ISO/IEC 27002:2015 «Інформаційні технології. Методи захисту. Звід практик щодо заходів інформаційної безпеки», затверджений наказом державного підприємства «Український науково-дослідний і навчальний центр проблем стандартизації, сертифікації та якості» від 18 грудня 2015 року № 193, (ISO/IEC 27002:2013; Cor 1:2014, IDT) (далі – ДСТУ ISO/IEC 27002);

ДСТУ ISO/IEC 27005:2015 «Інформаційні технології. Методи захисту. Управління ризиками інформаційної безпеки», затверджений наказом державного підприємства «Український науково-дослідний і навчальний

центр проблем стандартизації, сертифікації та якості» від 18 грудня 2015 року № 193, (ISO/IEC 27005:2011, IDT) (далі – ДСТУ ISO/IEC 27005).

6. У цих Вимогах терміни вживаються у таких значеннях:

адміністратор безпеки – роль співробітника, відповідального за СУІБ, кіберзахист (організовує проведення тестування вразливості ІТС тощо), захист інформації в ІТС, перегляд журналів аудиту;

адміністратор реєстрації – роль співробітника, відповідального за реєстрацію користувачів;

критичний компонент ІТС – компонент ІТС, захист якого передбачено вимогами безпеки або за результатами оцінки ризику;

несанкціоновані дії – несанкціонований доступ або спроба такого доступу до інформаційних ресурсів надавача або ВПР, вірусне ураження, вчинення інших дій, які можуть призвести до порушення цілісності, доступності та конфіденційності цих ресурсів;

оператор – роль співробітника, відповідального за експлуатацію засобів електронно-обчислювальної техніки ІТС та резервне копіювання даних;

приміщення надавача або ВПР (далі – приміщення) – приміщення, призначені для розміщення програмно-технічного комплексу (його складових), що використовується під час надання кваліфікованих електронних довірчих послуг;

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

системний адміністратор – роль співробітника, відповідального за обслуговування ІТС (налаштування, відновлення тощо), перегляд архівів;

службові приміщення (безпечна зона) – приміщення, доступ в які забезпечується із застосуванням організаційно-технічних заходів контролю (фізичний та логічний контроль);

спеціальні приміщення (зона підвищеної безпеки) – приміщення з обмеженим доступом, призначене для генерації, використання, зберігання та резервування особистих ключів надавача.

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», «Про засади державної регуляторної політики у сфері господарської діяльності» законодавства про електронні довірчі послуги та кіберзахист.

ІІ. Вимоги з управління інформаційною безпекою та захисту інформації

1. Організаційні питання

1.1. Захист інформації в ІТС та впровадження СУІБ забезпечується службою захисту інформації (далі – СЗІ) з дотриманням вимог Правил забезпечення захисту інформації в інформаційних, телекомунікаційних та інформаційно-телекомунікаційних системах, затверджених постановою Кабінету Міністрів України від 29 березня 2006 року № 373, та цих Вимог.

1.2. До складу СЗІ надавача входять:

1) посадова особа надавача, на яку наказом керівника надавача покладено обов'язки керівника служби захисту інформації;

2) адміністратор безпеки;

3) системний адміністратор.

1.3. При виконанні робіт із створення КСЗІ необхідно керуватися нормами НД ТЗІ 3.7-003-05 «Порядок проведення робіт із створення комплексної системи захисту інформації в інформаційно-телекомунікаційній системі», затвердженого наказом Департаменту спеціальних телекомунікаційних систем та захисту інформації Служби безпеки України від 08 листопада 2005 року № 125.

1.4. Вимоги до захисту інформації в ІТС визначаються власником ІТС у технічному завданні на створення КСЗІ (далі – ТЗ) і впроваджуються у вигляді організаційно-технічних рішень комплексів засобів захисту.

1.5. При виконанні робіт із створення СУІБ необхідно керуватися нормами ДСТУ ISO/IEC 27001, ДСТУ ETSI EN 319 401, ДСТУ ETSI EN 319 411-1, ДСТУ ETSI EN 319 411-2, ДСТУ ETSI EN 319 421 та цих Вимог. Заходи, передбачені ДСТУ ISO/IEC 27002, ДСТУ ISO/IEC 27005 є рекомендованими для впровадження, якщо інше не передбачено законодавством.

2. Політика інформаційної безпеки

2.1. Надавач повинен визначити політику інформаційної безпеки з дотриманням вимог пункту 6.3 ДСТУ ETSI EN 319 401 та цих Вимог.

2.2. Політика інформаційної безпеки затверджується керівником надавача.

2.3. Політика інформаційної безпеки доводиться до відома посадових осіб надавача та третіх осіб в частині що стосується (користувачі, органи з оцінки відповідності, регуляторні органи у сфері захисту інформації, електронних довірчих послуг, електронної ідентифікації, захисту персональних даних).

2.4. Політика інформаційної безпеки повинна бути задокументована, впроваджена та підтримувана.

2.5. Надавач несе повну відповідальність за недотримання процедур політики інформаційної безпеки, у тому числі при аутсорсингу.

2.6. У разі, якщо ВПР є окремою юридичною чи фізичною особою, надавач на підставі наказу або договору повинен визначити відповідальність ВПР та забезпечити контроль виконання ним встановлених законодавством процедур реєстрації, вимог з безпеки та захисту інформації.

3. Управління ризиками

3.1. Надавач запроваджує управління ризиками інформаційної безпеки з дотриманням вимог пункту 5 ДСТУ ETSI EN 319 401 та цих Вимог.

3.2. В рамках управління ризиками здійснюються визначення, аналіз та оцінки можливих ризиків при наданні електронних довірчих послуг з урахуванням економічних та технічних проблем.

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

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

3.5. Визначені надавачем заходи безпеки та операційні процедури, які необхідні для реалізації обраних ним заходів з управління ризиками, повинні бути зафіксовані в документах на СУІБ та в регламенті роботи надавача.

3.6. Управління ризиками та заходи з їх нейтралізації повинні регулярно переглядатися з періодичністю не менше ніж раз на рік.

3.7. Звіт з управління ризиками включає перелік можливих ризиків, результати їх оцінки, залишковий ризик. Звіт з управління ризиками затверджується керівником надавача.

4. Управління персоналом

4.1. Надавач запроваджує управління персоналом з дотриманням вимог пункту 7.2 ДСТУ ETSI EN 319 401, пункту 6.4.4 ДСТУ ETSI EN 319 411-1, вимог до кваліфікованих електронних довірчих послуг, встановлених Кабінетом Міністрів України, та цих Вимог.

4.2. Персонал повинен мати знання, досвід та кваліфікацію, необхідні для виконання функціональних обов'язків.

4.3. Персонал до моменту виконання посадових обов'язків повинен пройти навчання щодо захисту інформації та захисту персональних даних в навчальних закладах (установах та організаціях) та отримати підтверджувальні документи встановленого зразка.

4.4. Персонал, задіяний в забезпеченні надання послуг, повинен щорічно проходити практичні навчання з інформаційної безпеки, що включають вивчення нових загроз інформаційної безпеки та реагування на них.

4.5. До персоналу, що порушує політику або процедури надання послуг застосовуються відповідні дисциплінарні санкції.

4.6. Персонал повинен діяти в межах посадових інструкцій. В посадових інструкціях визначаються права та обов'язки за принципом найменшої привілеї.

4.7. У надавача є обов'язковими посади адміністратора безпеки, системного адміністратора, оператора, адміністратора реєстрації (разом далі – довірені ролі).

4.8. Персонал, що призначається на довірені ролі, повинен бути вільним від конфлікту інтересів, який може зашкодити неупередженості виконання функцій, що повинно бути підтверджено актом перевірки у встановленому надавачем порядку.

5. Управління активами

5.1. Надавач запроваджує управління активами з дотриманням вимог пункту 7.3 ДСТУ ETSI EN 319 401 та цих Вимог.

5.2. Надавач повинен забезпечити належний рівень захисту своїх активів, включаючи інформаційні активи.

5.3. Надавач повинен інвентаризувати всі інформаційні активи, їх класифікувати за оцінкою ризиків.

5.4. Конфіденційні дані, які втратили актуальність повинні бути знищені у спосіб, що не дозволяє їх відновити, зі складанням відповідного акту.

6. Управління доступом до інформаційних ресурсів ІТС

6.1. Надавач запроваджує управління доступом до інформаційних ресурсів ІТС з дотриманням вимог пункту 7.4 ДСТУ ETSI EN 319 401, пункту 6.4.3 ДСТУ ETSI EN 319 411-1 та цих Вимог.

6.2. Доступ до інформаційних ресурсів ІТС надається авторизованим співробітникам в межах виконання їх посадових обов'язків.

6.3. Надавач забезпечує управління обліковими записами співробітників: своєчасне надання, зміну, видалення прав доступу.

Використання системних комп'ютерних програм має бути обмеженим та контрольованим.

6.4. Співробітник повинен відповідати за свою діяльність зберігаючи пов'язанні журнали аудиту. Журнали аудиту повинні мати захист від несанкціонованого доступу, модифікації або знищення (руйнування) інформації.

6.5. Всі дії персоналу, пов'язані із генерацією пар ключів, формуванням сертифіката або зміною його статусу, повинні протоколюватися із забезпеченням захисту протоколів від несанкціонованого доступу, модифікації, знищення інформації.

6.6. Надавачем повинен бути передбачений захист ІТС від несанкціонованого доступу з боку зовнішніх (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 ІТС.

7. Управління засобами криптографічного захисту інформації

7.1. Надавач запроваджує управління засобами криптографічного захисту інформації (далі – КЗІ) з дотриманням вимог пункту 7.5 ДСТУ ETSI EN 319 401, вимог до кваліфікованих електронних довірчих послуг, та цих Вимог.

7.2. Засоби КЗІ повинні відповідати вимогам законодавства у сферах електронних довірчих послуг та КЗІ.

7.3. Надавач повинен забезпечити дотримання вимог з безпеки експлуатації засобів КЗІ протягом всього їх життєвого циклу, та вимог з управління ключами.

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

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

7.6. 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.

8. Управління ключами надавача

8.1. Генерація ключів надавача, їх резервування та відновлення, здійснюється визначеними керівником надавача особами (не менше двох) в межах їх функціональних обов'язків (далі – уповноважені особи) із забезпеченням розподілу таємниці (використання паролів доступу тощо) під контролем адміністратора безпеки.

8.2. Всі події, пов'язані із генерацією, використанням та знищенням ключів надавача, у тому числі даних доступу до них, повинні протоколюватися.

8.3. Особистий ключ надавача повинен розміщуватися на захищеному носії особистого ключа в складі програмно-апаратного або апаратного засобу КЗІ, яким здійснювалася генерація пари ключів, у спеціальному приміщенні.

8.4. Резервна копія особистого ключа зберігається у зашифрованому вигляді.

8.5. Посадові особи повинні зберігати дані доступу для управління ключами надавача у таємниці. Допускається резервування даних доступу для управління ключами надавача із забезпеченням захисту від несанкціонованого доступу.

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

8.7. Управління ключами надавача, призначеними для надання послуг формування, перевірки та підтвердження кваліфікованої електронної

позначки часу здійснюється з дотриманням вимог пункту 7.6 ДСТУ ETSI EN 319 421.

9. Управління фізичним доступом

9.1. Надавач запроваджує управління фізичним доступом з дотриманням вимог пункту 7.6 ДСТУ ETSI EN 319 401, пункту 6.4.2 ДСТУ ETSI EN 319 411-1 та цих Вимог. Під час надання послуг формування, перевірки та підтвердження кваліфікованої електронної позначки часу також застосовуються вимоги пункту 7.8 ДСТУ ETSI EN 319 421.

9.2. Доступ до критичних компонентів ІТС надається авторизованим співробітникам в межах виконання їх посадових обов'язків із застосуванням заходів контролю. До заходів контролю повинно бути віднесено визначення периметру безпеки, встановлення сигналізації.

9.3. Надавач повинен мінімізувати ризики, пов'язані із фізичною безпекою та вжити заходів для недопущення крадіжки, втрати та ушкодження обладнання, крадіжки та знищення (руйнування) інформації або інших дій, що можуть привести до виведення ІТС надавача із штатного режиму роботи.

9.4. Для спеціальних приміщень необхідно 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.

9.5. Вікна спеціального приміщення повинні бути:

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 надавача;

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

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

9.7. Для електроживлення технічних засобів, що розміщуються у спеціальних приміщеннях повинні бути встановленні пристрої безперервного електроживлення.

9.8. 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.

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

10. Управління операційною безпекою

10.1. Надавач запроваджує управління операційною безпекою з дотриманням вимог пункту 7.7 ДСТУ ETSI EN 319 401 та цих Вимог. Під час надання послуг формування, перевірки та підтвердження кваліфікованої електронної позначки часу також застосовуються вимоги пункту 7.9 ДСТУ ETSI EN 319 421.

10.2. Надавач здійснює придбання (з урахуванням потреби) та встановлення виключно ліцензійних комп'ютерних програм. Використання комп'ютерних програм здійснюється з дотриманням ліцензійної угоди її виробника.

10.3. Надавач в ІТС використовує загальносистемні технічні та програмні засоби, що мають вбудовані функції контролю цілісності,

автентифікації користувачів, ведення журналів подій, безпечного виконання операцій тощо.

10.4. Забороняється оновлення комп'ютерних програм, що забезпечують виконання процедур, пов'язаних з наданням послуг, з неідентифікованих та неавтентифікованих джерел, а також використання таких програм для оновлення електронних даних з порушеною цілісністю.

10.5. Надавач застосовує носії інформації захищені від пошкоджень та несанкціонованого доступу. Процедури управління носіями інформації повинні забезпечувати надійне зберігання інформації протягом встановленого строку.

10.6. Надавач здійснює заходи контролю використання носіїв інформації в ІТС, спрямованих запобіганню їх викраденню, пошкодженню, використанню понад експлуатаційного терміну, несанкціонованого доступу.

10.7. Надавач регулярно встановлює оновлення (патчі) безпеки. Забороняється застосування оновлень безпеки які містять уразливості та є нестабільними. Причини невикористання оновлень безпеки документуються.

11. Управління мережевою безпекою

11.1. Надавач запроваджує управління мережевою безпекою з дотриманням вимог пункту 7.8 ДСТУ ETSI EN 319 401 та цих Вимог. Під час надання послуг формування, перевірки та підтвердження кваліфікованої електронної позначки часу також застосовуються вимоги пункту 7.10 ДСТУ ETSI EN 319 421.

11.2. Надавач (ВПР) визначає порядок взаємодії між робочими станціями та системами (службами) та вживає заходи захисту ІТС від кібератак.

11.3. Заходи захисту ІТС від кібератак включають розподілення ІТС надавача на сегменти (підсистеми) на основі оцінки ризику з урахуванням функціональних, логічних та фізичних (включаючи місцезнаходження) взаємозв'язків між робочими станціями та системами (службами). Для всіх технічних та програмних засобів, розташованих у одному сегменті

застосовуються однакові елементи контролю безпеки. Доступ і зв'язки між сегментами обмежуються тільки необхідними для правильного функціонування ІТС, а необов'язкові підключення повинні бути явно заборонені або дезактивовані.

11.4. Локальний сегмент ІТС, який забезпечує управління надання послугами, та сегмент ІТС, який забезпечує взаємодію з користувачами, повинні бути розділені. Робочі станції, що використовуються для управління безпекою не повинні використовуватися для інших цілей. ІТС надавача має бути відокремлена від середовищ розробки та тестування.

11.5. Конфіденційна інформація та персональні дані користувача у разі передавання зовнішніми комп'ютерними мережами повинна бути зашифрована.

11.6. Для ІТС надавача повинно здійснюватися регулярне сканування вразливостей на загальнодоступній та приватній (за наявності) зовнішніх мережевих адресах з періодичністю не менше ніж один раз на рік. На етапі введення ІТС надавача в експлуатацію або, за необхідності, після проведення її модернізації, здійснюється тестування на проникнення.

11.7. Факт проведення сканування вразливостей або тестування на проникнення документується із складанням звіту.

11.8. Надавач (ВПР) здійснює резервне копіювання даних, необхідних для функціонування ІТС, у територіально відокремлених місцях із забезпеченням належного захисту цих даних.

12. Управління інцидентами

12.1. Надавач (ВПР) запроваджує управління інцидентами в ІТС з дотриманням вимог пункту 7.9 ДСТУ ETSI EN 319 401, пункту 6.4.8 ДСТУ ETSI EN 319 411-1 та цих Вимог.

12.2. Для управління інцидентами в ІТС надавач забезпечує функціонування системи моніторингу, що збирає та аналізує інформацію про стан критичних компонентів ІТС, в тому числі про вимкнення, запуск, перезапуск, доступність та рівень навантаження таких компонентів.

12.3. Система моніторингу має виявляти та повідомляти сигналом тривоги аномальну системну активність, що вказує на потенційне порушення системи безпеки, включаючи вторгнення в ІТС.

12.4. 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.

12.5. Надавач повинен повідомити контролюючий орган про порушення вимог з безпеки та захисту інформації, встановленні у позиції третій частини п'ятої статті 33 Закону України «Про електронні довірчі послуги» протягом 24 годин після виявлення порушення.

12.6. 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 не пізніше двох годин з моменту, коли стало відомо про порушення, повідомити таку фізичну або юридичну особу.

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

13. Управління доказами та архівами

13.1. Надавач (ВПР) запроваджує управління доказами та архівами з дотриманням вимог пункту 7.10 ДСТУ ETSI EN 319 401, пунктів 6.4.5, 6.4.6 ДСТУ ETSI EN 319 411-1 та цих Вимог. Під час надання послуг формування, перевірки та підтвердження кваліфікованої електронної позначки часу також застосовуються вимоги пункту 7.12 ДСТУ ETSI EN 319 421.

13.2. Надавач забезпечує збір доказів про події, що відбуваються в ІТС, у спосіб ведення журналів аудиту подій.

13.3. У журналах аудиту подій реєструються події таких типів:

1) спроби створення, знищення, встановлення паролів, зміни прав доступу в ІТС тощо;

2) заміни технічних засобів ІТС та пар ключів;

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

4) спроби несанкціонованого доступу до ІТС;

5) надання доступу персоналу до ІТС;

6) зміни системних конфігурацій та технічне обслуговування ІТС;

7) збої в роботі ІТС;

8) інші події, необхідні для збору доказів.

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

13.5 Журнали аудиту подій резервуються та переглядаються адміністратором безпеки не рідше одного разу на тиждень в рамках чого перевіряється наявність несанкціонованої модифікації та вивчаються події.

13.6. Час, що зазначається, у журналі аудиту подій повинен бути синхронізований із Всесвітнім координованим часом з точністю до секунди.

13.7. Журнали аудиту подій повинні бути захищенні від неавторизованого перегляду, модифікації і знищення.

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

13.9. Надавач зберігає журнали аудиту подій на місці їх створення протягом 10 років, після чого забезпечує їх передачу на архівне зберігання.

13.10. Резервні копії кваліфікованих сертифікатів відкритих ключів та журналів аудиту подій повинні зберігатися в будівлі окремо розташованій від

будівлі ІТС надавача із забезпеченням їх захисту від несанкціонованого доступу.

14. Управління безперервністю надання послуг

14.1. Надавач (ВПР) запроваджує управління безперервністю надання послуг з дотриманням вимог пункту 7.11 ДСТУ ETSI EN 319 401, пункту 6.4.8 ДСТУ ETSI EN 319 411-1, вимог до кваліфікованих електронних довірчих послуг, встановлених Кабінетом Міністрів України, та цих Вимог. Під час надання послуг формування, перевірки та підтвердження кваліфікованої електронної позначки часу також застосовуються вимоги пункту 7.13 ДСТУ ETSI EN 319 421.

14.2. Надавач повинен затвердити та підтримувати в актуальному стані інструкцію з безперервності надання послуг при настанні надзвичайних подій, в якій визначити дії персоналу та строки виконання заходів з відновлення діяльності.

15. Управління припиненням надання послуг

15.1. Надавач (ВПР) запроваджує управління припиненням надання послуг з дотриманням вимог пункту 7.12 ДСТУ ETSI EN 319 401, пункту 6.4.9 ДСТУ ETSI EN 319 411-1, вимог до кваліфікованих електронних довірчих послуг та цих Вимог. Під час надання послуг формування, перевірки та підтвердження кваліфікованої електронної позначки часу також застосовуються вимоги пункту 7.14 ДСТУ ETSI EN 319 421.

15.2. Надавач повинен затвердити та підтримувати в актуальному стані план з припинення діяльності, в якому визначити порядок та строки виконання заходів з припинення діяльності.

Директор Департаменту захистуінформації
Адміністрації Державної служби спеціального
зв'язку та захисту інформації України Андрій Пушкарьов

ПОЯСНЮВАЛЬНА ЗАПИСКА

до проекту наказу Адміністрації Державної служби спеціального зв'язку та захисту інформації України «Про встановлення вимог з безпеки та захисту інформації до кваліфікованих надавачів електронних довірчих послуг та їхніх відокремлених пунктів реєстрації»

Мета: підвищення рівня довіри фізичних і юридичних осіб до кваліфікованих електронних довірчих послуг, безпеки та захисту інформації при їх наданні, шляхом встановлення відповідних вимог до кваліфікованих надавачів електронних довірчих послуг та їхніх відокремлених пунктів реєстрації.

1. Підстава розроблення проекту акта

Проект наказу Адміністрації Державної служби спеціального зв'язку та захисту інформації України «Про встановлення вимог з безпеки та захисту інформації до кваліфікованих надавачів електронних довірчих послуг та їхніх відокремлених пунктів реєстрації» (далі – проект наказу) розроблено на виконання:

абзацу третього частини другої статті 8, абзацу третього частини другої статті 13, абзацу третього пункту 8 розділу VII «Прикінцеві та перехідні положення» Закону України «Про електронні довірчі послуги»;

пункту 37 частини першої статті 14 Закону України «Про Державну службу спеціального зв'язку та захисту інформації України»;

підпункту 2 пункту 3 Положення про Адміністрацію Державної служби спеціального зв'язку та захисту інформації України, затвердженого постановою Кабінету Міністрів України від 3 вересня 2014 року № 411;

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

2. Обгрунтування необхідності прийняття акта

Необхідність прийняття проекту наказу полягає у потребі врегулювання питань забезпечення належного рівня безпеки та захисту інформації при наданні кваліфікованих електронних довірчих послуг, створення умов для надання кваліфікованих електронних довірчих послуг, гармонізованих із положеннями актів законодавства Європейського Союзу, а саме:

Регламенту (ЄС) № 910/2014 Європейського Парламенту та Ради від 23 липня 2014 року щодо електронної ідентифікації та довірчих послуг для

цілей електронних транзакцій на внутрішньому ринку, що скасовує Директиву 1999/93/ЄС Європейського Парламенту та Ради;

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

Прийняття проекту наказу відповідає зобов'язанням України у зв'язку з ратифікацією Угоди про асоціацію між Україною, з однієї сторони, та Європейським Союзом, Європейським співтовариством з атомної енергії і їхніми державами-членами, з іншої сторони, зокрема пов'язаним із вжиттям заходів, спрямованих на створення системи контролю за додержанням законодавства та забезпечення організаційної спроможності органу, відповідального за здійснення контролю за дотриманням законодавства у сфері електронних довірчих послуг.

3. Суть проекту акта

Проектом наказу пропонується визначити організаційно-методологічні, технічні та технологічні вимоги безпеки та захисту інформації, яких повинні дотримуватись кваліфіковані надавачі електронних довірчих послуг, їх відокремлені пункти реєстрації під час надання кваліфікованих електронних довірчих послуг їх користувачам, а саме вимоги до:

забезпечення безпеки інформаційних ресурсів надавача кваліфікованих електронних довірчих послуг та його відокремлених пунктів реєстрації шляхом впровадження системи управління інформаційною безпекою та комплексної системи захисту інформації інформаційно-телекомунікаційної системи, з підтвердженою відповідністю;

персоналу надавача кваліфікованих електронних довірчих послуг та його відокремлених пунктів реєстрації, зокрема щодо наявності відповідної кваліфікації (підтверджувальних документів встановленого зразка про навчання щодо захисту інформації та захисту персональних даних, а також щорічного проходження практичних навчань з інформаційної безпеки);

розподілу персоналу надавача кваліфікованих електронних довірчих послуг та його відокремлених пунктів реєстрації за встановленими ролями;

спеціальних приміщень призначених для генерації, використання, зберігання та резервування особистих ключів надавача кваліфікованих електронних довірчих послуг;

управління ризиками та заходів з їх нейтралізації, які повинні переглядатися не рідше одного разу на рік.

Способом врегулювання зазначених питань є затвердження відповідного проекту наказу.

4. Правові аспекти

Правовими підставами розроблення проекту наказу є:

Закон України «Про електронні довірчі послуги»;

Закону України «Про Державну службу спеціального зв'язку та захисту інформації України»;

Положення про Адміністрацію Державної служби спеціального зв'язку та захисту інформації України, затверджене постановою Кабінету Міністрів України від 3 вересня 2014 року № 411;

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

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

5. Фінансово-економічне обґрунтування

Виходячи з проведеної фінансово-економічної оцінки, реалізація проекту наказу потребуватиме додаткових фінансових витрат з державного бюджету у зв'язку з необхідністю підвищення кваліфікації персоналу кваліфікованих надавачів електронних довірчих послуг та посиленням заходів захисту інформаційно-телекомунікаційних систем діючих акредитованих центрів сертифікації ключів.

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

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

З огляду на зазначене реалізація проекту наказу потребуватиме додаткових фінансових витрат з державного бюджету для 6 акредитованих

центрів сертифікації ключів, які фінансуються за рахунок державного бюджету та мають намір надавати кваліфіковані електронні довірчі послуги.

Вартість реалізації одним акредитованим центром сертифікації ключів (державного органу або суб'єкта господарювання) заходів передбачених проектом наказу у 2019 році щонайменше складатиме 356 600,00 грн. (зведені фінансово-економічні розрахунки до проекту наказу наведено у аналізі регуляторного впливу, опублікованому на офіційному веб-сайті Адміністрація Держспецзв'язку у розділі «регуляторна діяльність»).

6. Прогноз впливу

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

З огляду на зазначене відповідно до статті 8 Закону України «Про засади державної регуляторної політики у сфері господарської діяльності» необхідне проведення аналізу регуляторного впливу проекту наказу.

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

За предметом правового регулювання проект наказу не матиме впливу на:

розвиток регіонів;

громадське здоров'я;

екологію та навколишнє природне середовище.

7. Позиція заінтересованих сторін

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

Прогноз впливу реалізації акта на ключові інтереси заінтересованих сторін наведено у аналізі регуляторного впливу, опублікованому на офіційному веб-сайті Держспецзв'язку у розділі «регуляторна діяльність.

За предметом правового регулювання проект наказу не стосується:

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

соціально-трудової сфери;

прав осіб з інвалідністю;

сфери наукової та науково-технічної діяльності.

8. Громадське обговорення

З метою проведення громадського обговорення проект наказу розміщено на офіційному веб-сайті Держспецзв'язку.

9. Позиція заінтересованих органів

Проект наказу підлягає погодженню з Міністерством економічного розвитку і торгівлі України, Міністерством фінансів України, Міністерством юстиції України, Державною регуляторною службою України, Державним агентством з питань електронного урядування України, Антимонопольним комітетом України.

10. Правова експертиза

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

11. Запобігання дискримінації

У проекті наказу відсутні положення, які містять ознаки дискримінації.

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

Проект наказу не потребує проведення громадської антидискримінаційної експертизи.

12. Запобігання корупції

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

Проект наказу не потребує проведення громадської антикорупційної експертизи.

13. Прогноз результатів

Прийняття проекту наказу дозволить:

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

забезпечити відповідність вимог з безпеки та захисту інформації у сфері надання електронних довірчих послуг європейським та міжнародним стандартам;

забезпечити захист належний рівень захисту інформації та персональних даних, що обробляються під час надання електронних довірчих послуг;

забезпечити здійснення контролю безпеки та захисту інформації при наданні електронних довірчих послуг.

Голова Державної служби спеціального зв'язку та захисту інформації України **Леонід Євдоченко**

«17» 09 2018 року

АНАЛІЗ РЕГУЛЯТОРНОГО ВПЛИВУ
проекту наказу Адміністрації Державної служби спеціального зв'язку та захисту інформації України «Про встановлення вимог з безпеки та захисту інформації до кваліфікованих надавачів електронних довірчих послуг та їхніх відокремлених пунктів реєстрації»

І. Визначення проблеми

Проект наказу Адміністрації Державної служби спеціального зв'язку та захисту інформації України «Про встановлення вимог з безпеки та захисту інформації до кваліфікованих надавачів електронних довірчих послуг та їхніх відокремлених пунктів реєстрації» (далі – проект наказу) розроблено на виконання абзацу третього частини другої статті 8, абзацу третього частини другої статті 13, абзацу третього пункту 8 розділу VII «Прикінцеві та перехідні положення» Закону України «Про електронні довірчі послуги» (далі – Закон) та пункту 37 частини першої статті 14 Закону України «Про Державну службу спеціального зв'язку та захисту інформації України».

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

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

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

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

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

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

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

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

підвищення рівня безпеки та захисту інформації при наданні кваліфікованих електронних довірчих послуг;

покращення якості надання кваліфікованих електронних довірчих послуг;

підвищення рівня довіри до кваліфікованих електронних довірчих послуг.

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

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

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

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

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

створення системи контролю за додержанням законодавства та забезпечення організаційної спроможності органу, відповідального за здійснення такого контролю у сфері електронних довірчих послуг;

дерегуляцію і розвиток підприємництва та конкуренції;

розвиток галузей електронної торгівлі, науки, технологій та інновацій.

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

II. Цілі державного регулювання

Проект наказу розроблено з метою підвищення рівня довіри фізичних і юридичних осіб до кваліфікованих електронних довірчих послуг, безпеки та захисту інформації при їх наданні, шляхом встановлення відповідних вимог до кваліфікованих надавачів електронних довірчих послуг та їхніх відокремлених пунктів реєстрації.

III. Визначення та оцінка альтернативних способів досягнення цілей

1. Визначення альтернативних способів

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

Вид альтернативи	Опис альтернативи
Альтернатива 1 Прийняття проекту наказу	Прийняття проекту наказу передбачає продовження та подальший розвиток реформи законодавства у сфері електронного цифрового підпису, розпочатої у зв'язку з прийняттям Закону України «Про електронні довірчі послуги», шляхом становлення законодавства у сфері електронних довірчих послуг. Так, проектом наказу пропонується визначити організаційно-методологічні, технічні та технологічні вимоги безпеки та захисту інформації, яких повинні дотримуватись кваліфіковані надавачі електронних довірчих послуг, їх відокремлені пункти реєстрації під час надання кваліфікованих електронних довірчих послуг їх користувачам, а саме вимоги до: забезпечення безпеки інформаційних ресурсів надавача кваліфікованих електронних довірчих послуг та його відокремлених пунктів реєстрації шляхом впровадження системи управління інформаційною безпекою та комплексної системи захисту інформації інформаційно-телекомунікаційної системи, з підтвердженою відповідністю; персоналу надавача кваліфікованих електронних довірчих послуг та його відокремлених пунктів реєстрації, зокрема щодо наявності відповідної кваліфікації (підтверджувальних документів встановленого зразка про навчання щодо захисту інформації та захисту персональних даних, а також щорічного проходження практичних навчань з інформаційної безпеки); розподілу персоналу надавача кваліфікованих електронних довірчих послуг та його відокремлених пунктів реєстрації за встановленими ролями; спеціальних приміщень призначених для генерації, використання, зберігання та резервування особистих ключів надавача кваліфікованих електронних довірчих послуг; управління ризиками та заходів з їх нейтралізації, які повинні переглядатися не рідше одного разу на рік;

Альтернатива 2 Відсутність регулювання	Відсутність регулювання передбачає залишення існуючого стану справ та зупинення реформи законодавства у сфері електронного цифрового підпису, зокрема ігнорування заходів щодо: 1) виконання зобов'язань України, пов'язаних з ратифікацією Угоди про асоціацію між Україною, з однієї сторони, та Європейським Союзом, Європейським співтовариством з атомної енергії і їхніми державами-членами, з іншої сторони, спрямованих на: забезпечення відповідності вимог до надання електронних довірчих послуг європейським та міжнародним стандартам; створення системи контролю за додержанням законодавства та забезпечення організаційної спроможності органу, відповідального за здійснення такого контролю у сфері електронних довірчих послуг; дерегуляцію і розвиток підприємництва та конкуренції; розвиток галузей електронної торгівлі, науки, технологій та інновацій. 2) гармонізації українського законодавства із законодавством Європейського Союзу, а саме з положеннями Регламенту (ЄС) № 910/2014 Європейського Парламенту та Ради від 23 липня 2014 року щодо електронної ідентифікації та довірчих послуг для цілей електронних транзакцій на внутрішньому ринку, що скасовує Директиву 1999/93/ЄС Європейського Парламенту та Ради, та імплементаційних рішень Європейського Союзу, виданих на виконання зазначеного Регламенту; 3) виконання абзацу третього частини другої статті 8, абзацу третього частини другої статті 13, абзацу третього пункту 8 розділу VII «Прикінцеві та перехідні положення» Закону України «Про електронні довірчі послуги»; Крім того, зазначений альтернативний спосіб державного регулювання призведе до збільшення вразливості кваліфікованих надавачів електронних довірчих послуг як об'єкта критичної інформаційної інфраструктури до кіберзагроз, не дасть можливості забезпечити належний рівень якості надання кваліфікованих електронних довірчих послуг і захисту при обробці персональних даних користувачів та несе потенційну загрозу зменшення рівня довіри до роботи кваліфікованих надавачів електронних довірчих послуг на національному рівні, а особливо на рівні транскордонної взаємодії.

2. Оцінка вибраних альтернативних способів досягнення цілей

Оцінка впливу на сферу інтересів держави:

Вид альтернативи	Вигоди	Витрати
Альтернатива 1 Прийняття проекту наказу	Прийняття проекту наказу матиме такий вплив на інтереси держави: підвищення рівня безпеки та захисту інформації при наданні кваліфікованих електронних довірчих послуг; покращення якості надання кваліфікованих електронних довірчих послуг; підвищення рівня довіри до кваліфікованих електронних довірчих послуг; популяризацію електронного документообігу та використання засобів електронної ідентифікації зокрема, для отримання адміністративних послуг в електронній формі; зменшення витрат держави на комунікації з фізичними та юридичними особами.	Прийняття проекту наказу: потребуватиме збільшення видатків з державного бюджету внаслідок запровадження додаткових організаційно-методологічних, технічних та технологічних умов діяльності кваліфікованих надавачів електронних довірчих послу, що фінансуються з державного бюджету; може призвести до збільшення вартості кваліфікованих електронних довірчих послуг для їх користувачів (в тому числі органів державної влади) внаслідок збільшення витрат кваліфікованих надавачів електронних довірчих послуг, пов'язаних із запровадженням додаткових організаційно-методологічних, технічних та технологічних умов діяльності з метою покращення якості та забезпечення належного рівня захисту інформації при наданні кваліфікованих електронних довірчих послуг.
Альтернатива 2 Відсутність регулювання	Відсутність регулювання означає залишення існуючого стану справ, що не передбачає жодних вигод для держави	Відсутність регулювання означає залишення існуючого стану справ, що не матиме такого впливу на інтереси держави: підвищення рівня

		безпеки та захисту інформації при наданні кваліфікованих електронних довірчих послуг; покращення якості надання кваліфікованих електронних довірчих послуг; підвищення рівня довіри до кваліфікованих електронних довірчих послуг; популяризацію електронного документообігу та використання засобів електронної ідентифікації зокрема, для отримання адміністративних послуг в електронній формі; зменшення витрат держави на комунікації з фізичними та юридичними особами.

Оцінка впливу на сферу інтересів громадян:

Вид альтернативи	Вигоди	Витрати
Альтернатива 1 Прийняття проекту наказу	Прийняття проекту наказу матиме такий вплив на інтереси громадян: підвищення рівня безпеки та захисту інформації при наданні кваліфікованих електронних довірчих послуг; покращення якості надання кваліфікованих електронних довірчих послуг; підвищення рівня довіри до кваліфікованих електронних довірчих послуг; популяризацію електронного документообігу та використання засобів електронної ідентифікації зокрема, для отримання адміністративних послуг в електронній формі;	Прийняття проекту наказу може призвести до збільшення вартості кваліфікованих електронних довірчих послуг для їх користувачів (в тому числі громадян) внаслідок збільшення витрат кваліфікованих надавачів електронних довірчих послуг, пов'язаних із запровадженням додаткових організаційно-методологічних, технічних та технологічних умов діяльності з метою покращення якості та забезпечення належного рівня захисту інформації при наданні кваліфікованих електронних довірчих послуг.

	зменшення витрат держави на комунікації з фізичними та юридичними особами.	
Альтернатива 2 Відсутність регулювання	Відсутність регулювання означає залишення існуючого стану справ, що не передбачає жодних вигод для громадян	Відсутність регулювання означає залишення існуючого стану справ, що не матиме такого впливу на інтереси громадян: підвищення рівня безпеки та захисту інформації при наданні кваліфікованих електронних довірчих послуг; покращення якості надання кваліфікованих електронних довірчих послуг; підвищення рівня довіри до кваліфікованих електронних довірчих послуг; популяризацію електронного документообігу та використання засобів електронної ідентифікації зокрема, для отримання адміністративних послуг в електронній формі; зменшення витрат держави на комунікації з фізичними та юридичними особами.

Оцінка впливу на сферу інтересів суб'єктів господарювання:

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

Вид альтернативи	Вигоди	Витрати
Альтернатива 1 Прийняття проекту наказу	Прийняття проекту наказу матиме такий вплив на інтереси суб'єктів	Прийняття проекту наказу призведе до збільшення витрат суб'єкта

	господарювання: покращення якості надання кваліфікованих електронних довірчих послуг; підвищення рівня довіри до кваліфікованих електронних довірчих послуг; збільшення кількості користувачів кваліфікованих електронних довірчих послуг; збільшення прибутку суб'єкта господарювання	господарювання внаслідок запровадження додаткових організаційно-методологічних, технічних та технологічних умов діяльності з метою покращення якості та забезпечення належного рівня захисту інформації при наданні кваліфікованих електронних довірчих послуг.
Альтернатива 2 Відсутність регулювання	Відсутність регулювання означає залишення існуючого стану справ, що не передбачає жодних вигод для суб'єктів господарювання	Відсутність регулювання означає залишення існуючого стану справ, що не матиме такого впливу на інтереси суб'єктів господарювання: покращення якості надання кваліфікованих електронних довірчих послуг; підвищення рівня довіри до кваліфікованих електронних довірчих послуг; збільшення кількості користувачів кваліфікованих електронних довірчих послуг; збільшення прибутку суб'єкта господарювання.

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

Порядковий номер	Витрати	За перший рік	За п'ять років
1.	**Витрати на придбання основних фондів, обладнання та приладів, сервісне обслуговування, навчання / підвищення кваліфікації персоналу тощо, гривень:**	**145 700,00**	**160 700,00**
1.1.	проведення модернізації комплексної системи захисту інформації в інформаційно-телекомунікаційній системі кваліфікованого надавача електронних довірчих послуг (придбання обладнання, приладів та ліцензійного програмного	130 700,00	130 700,00

	забезпечення)		
1.2.	підвищення кваліфікації найманих працівників кваліфікованого надавача електронних довірчих послуг (5 осіб х 3 000,00 грн) у сферах інформаційних технологій, захисту інформації або кібербезпеки та захисту персональних даних	15 000,00	30 000,00
2.	**Витрати, пов'язані із веденням обліку, підготовкою та поданням звітності державним органам, гривень**	**200,00**	**1 000,00**
2.1.	підготовка щорічного звіту для контролюючого органу про діяльність кваліфікованого надавача електронних довірчих послуг	200,00	1 000,00
3.	**Витрати, пов'язані з адмініструванням заходів державного нагляду (контролю) (перевірок, штрафних санкцій, виконання рішень/приписів тощо), гривень**	**2 200,00**	**4 400, 00**
3.1.	Витрати пов'язані з адмініструванням виїзних перевірок	2 200,00	4 400, 00
4.	**Витрати на отримання адміністративних послуг (дозволів, ліцензій, сертифікатів, атестатів, погоджень, висновків, проведення незалежних/обов'язкових експертиз, сертифікації, атестації тощо) та інших послуг (проведення наукових, інших експертиз, страхування тощо), гривень:**	**162 800,00**	**163 000,00**
4.1.	погодження регламенту роботи кваліфікованого надавача електронних довірчих послуг	200,00	400,00
4.2.	проведення додаткової державної експертизи комплексної системи захисту інформації інформаційно-телекомунікаційної системи кваліфікованого надавача електронних довірчих послуг	162 600,00	162 600,00
5.	**Витрати на оборотні активи (матеріали, канцелярські товари тощо), гривень**	**1 000,00**	**5 000,00**
6.	**Витрати, пов'язані із наймом додаткового персоналу, гривень:**	**44 700,00**	**223 500,00**
6.1.	найм кваліфікованим надавачем електронних довірчих послуг додаткового	44 700,00	223 500,00

	персоналу на посади з роллю адміністратора безпеки (щонайменше 1) у зв'язку із введенням додаткових обов'язків (мінімальна заробітна плата у місячному розмірі: з 1 січня 2018 року – 3723,00 гривні)		
7	**РАЗОМ (сума рядків: 1 + 2 + 3 + 4 + 5 + 6), гривень**	**356 600,00**	**557 600,00**

Сумарні витрати за альтернативами	Сума витрат, гривень
Альтернатива 1 Прийняття проекту наказу	356 600,00
Альтернатива 2 Відсутність регулювання	0,00

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

IV. Вибір найбільш оптимального альтернативного способу досягнення цілей

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

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

Рейтинг результативності (досягнення цілей під час вирішення проблеми)	Бал результативності (за чотирибальною системою оцінки)	Коментарі щодо присвоєння відповідного бала
Альтернатива 1 Прийняття проекту наказу	4	Прийняття проекту наказу сприятиме: покращенню якості надання кваліфікованих електронних довірчих послуг; підвищенню рівня довіри до кваліфікованих електронних довірчих послуг; збільшенню кількості користувачів кваліфікованих

		електронних довірчих послуг; збільшенню прибутку суб'єктів господарювання
Альтернатива 2 Відсутність регулювання	1	Відсутність регулювання передбачає залишення існуючого стану справ та зупинення реформи законодавства у сфері електронного цифрового підпису

Рейтинг результативності	Вигоди (підсумок)	Витрати (підсумок)	Обґрунтування відповідного місця альтернативи у рейтингу
Альтернатива 1 Прийняття проекту наказу	Прийняття проекту наказу сприятиме: підвищенню рівня безпеки та захисту інформації при наданні кваліфікованих електронних довірчих послуг; покращенню якості надання кваліфікованих електронних довірчих послуг; підвищенню рівня довіри до кваліфікованих електронних довірчих послуг; збільшенню кількості користувачів кваліфікованих електронних довірчих послуг; збільшенню прибутку суб'єкта господарювання; популяризації електронного	Прийняття проекту наказу може призвести до збільшення вартості кваліфікованих електронних довірчих послуг для їх користувачів внаслідок збільшення витрат кваліфікованих надавачів електронних довірчих послуг, пов'язаних із запровадженням додаткових організаційно-методологічних, технічних та технологічних умов діяльності з метою покращення якості та забезпечення належного рівня захисту інформації при наданні кваліфікованих електронних довірчих послуг.	Цілі, визначені стратегічним документами досягнуті

	документообігу та використання засобів електронної ідентифікації зокрема, для отримання адміністративних послуг в електронній формі; зменшення витрат держави на комунікації з фізичними та юридичними особами.		
Альтернатива 2 Відсутність регулювання	Відсутність регулювання означає залишення існуючого стану справ, що не передбачає жодних вигод для держави, громадян та суб'єктів господарювання	Відсутність регулювання означає залишення існуючого стану справ, що не передбачає жодних витрат для держави, громадян та суб'єктів господарювання	Недосягнення цілей, визначених стратегічними документами

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

Основними механізмами, які забезпечують розв'язання визначеної проблеми, є встановлення вимог з безпеки та захисту інформації до кваліфікованих надавачів електронних довірчих послуг та їхніх відокремлених пунктів реєстрації, шляхом прийняття відповідного наказу Адміністрації Державної служби спеціального зв'язку та захисту інформації України.

Заходами, спрямованими на розв'язання визначеної проблеми є:

розробка проекту наказу;

громадське обговорення проекту наказу;

погодження проекту наказу із заінтересованими органами;

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

подання проекту наказу на державну реєстрацію до Міністерства юстиції України;

прийняття наказу Адміністрації Державної служби спеціального зв'язку та захисту інформації України «Про встановлення вимог з безпеки та захисту інформації до кваліфікованих надавачів електронних довірчих послуг та їхніх відокремлених пунктів реєстрації».

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

Бюджетні витрати на адміністрування регулювання для суб'єктів великого і середнього підприємництва:

Процедура регулювання суб'єктів великого і середнього підприємництва (розрахунок на одного типового суб'єкта господарювання)	Планові витрати часу на процедуру	Вартість часу співробітника органу державної влади відповідної категорії (заробітна плата)	Оцінка кількості процедур за рік, що припадають на одного суб'єкта	Оцінка кількості суб'єктів, що підпадають під дію процедури регулювання	Витрати на адміністрування регулювання (за рік), гривень
1. Облік суб'єкта господарювання, що перебуває у сфері регулювання	**2 робочі дні**	**400,00 грн за робочий день (з розрахунку 9 000,00 грн за місяць)**	**2**	**24**	**800,00**
Адміністрація Державної служби спеціального зв'язку та захисту інформації України	1 робочий день	400,00 грн за робочий день (з розрахунку 9 000,00 грн за місяць)	1	24	400,00
Міністерство юстиції України	1 робочий день	400,00 грн за робочий день (з розрахунку 9 000,00 грн за місяць)	1	24	400,00
2. Поточний контроль за суб'єктом господарювання, що перебуває у сфері регулювання, у тому числі:	**15 робочих днів**	**400,00 грн за робочий день (з розрахунку 9 000,00 грн за місяць)**	**2**	**24**	**6 000,00**
безвиїзний нагляд (Адміністрація Державної служби спеціального зв'язку та захисту інформації України)	2 робочих дні	400,00 грн за робочий день (з розрахунку 9 000,00 грн за місяць)	1	24	800,00

виїзні перевірки (Адміністрація Державної служби спеціального зв'язку та захисту інформації України)	10 робочих днів	400,00 грн за робочий день (з розрахунку 9 000,00 грн за місяць)	1	24	4 000,00
3. Підготовка, затвердження та опрацювання одного окремого акта про порушення вимог регулювання (Адміністрація Державної служби спеціального зв'язку та захисту інформації України)	**1 робочий день**	**400,00 грн за робочий день (з розрахунку 9 000,00 грн за місяць)**	**1**	**24**	**400,00**
4. Реалізація одного окремого рішення щодо порушення вимог регулювання	**2 робочі дні**	**400,00 грн за робочий день (з розрахунку 9 000,00 грн за місяць)**	**2**	**24**	**800,00**
Адміністрація Державної служби спеціального зв'язку та захисту інформації України	1 робочий день	400,00 грн за робочий день (з розрахунку 9 000,00 грн за місяць)	1	24	400,00
Міністерство юстиції України	1 робочий день	400,00 грн за робочий день (з розрахунку 9 000,00 грн за місяць)	1	24	400,00
5. Оскарження одного окремого рішення суб'єктами господарювання	**2 робочі дні**	**400,00 грн за робочий день (з розрахунку 9 000,00 грн за місяць)**	**2**	**24**	**800,00**
Адміністрація Державної служби спеціального зв'язку та захисту	1 робочий день	400,00 грн за робочий день (з розрахунку 9 000,00 грн за місяць)	1	24	400,00

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

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

VII. Обгрунтування запропонованого строку дії регуляторного акта

Строк дії проекту наказу не обмежений у часі.

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

Проект наказу набирає чинності з моменту опублікування, але не раніше дня набрання чинності Законом України «Про електронні довірчі послуги».

VIII. Визначення показників результативності дії регуляторного акта

Показники результативності дії регуляторного акта:

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

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

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

рівень поінформованості суб'єктів господарювання та/або фізичних осіб з основних положень акта (високий, – оскільки проект наказу розміщено на офіційному веб-сайті Адміністрації Державної служби спеціального зв'язку та захисту інформації України;

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

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

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

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

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

Базове відстеження результативності проекту наказу буде здійснюватись через рік після набрання чинності зазначеним наказом, оскільки планується використовувати статистичний метод відстеження та статистичні дані.

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

Періодичні відстеження планується здійснювати раз на три роки, починаючи з дня проведення повторного відстеження. Установлені показники

результативності акта порівнюватимуться із значеннями аналогічних показників, що встановлені під час повторного відстеження.

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

Виконавець заходів з відстеження результативності проекту наказу – Адміністрація Державної служби спеціального зв'язку та захисту інформації України.

Голова Державної служби спеціального зв'язку та захисту інформації України **Леонід Євдоченко**

«17» 09 2018 року

Повідомлення про оприлюднення
проекту наказу Адміністрації Державної служби спеціального зв'язку та захисту інформації України «Про встановлення вимог з безпеки та захисту інформації до кваліфікованих надавачів електронних довірчих послуг та їхніх відокремлених пунктів реєстрації»

1. Стислий виклад змісту проекту акта

Проект наказу Адміністрації Державної служби спеціального зв'язку та захисту інформації України «Про встановлення вимог з безпеки та захисту інформації до кваліфікованих надавачів електронних довірчих послуг та їхніх відокремлених пунктів реєстрації», підготовлено на виконання абзацу третього частини другої статті 8, абзацу третього частини другої статті 13, абзацу третього пункту 8 розділу VII «Прикінцеві та перехідні положення» Закону України «Про електронні довірчі послуги».

Проектом наказу пропонується визначити організаційно-методологічні, технічні та технологічні вимоги безпеки та захисту інформації, яких повинні дотримуватись кваліфіковані надавачі електронних довірчих послуг, їх відокремлені пункти реєстрації під час надання кваліфікованих електронних довірчих послуг їх користувачам.

2. Адреси для зауважень та пропозицій до проекту акта

Пропозиції та зауваження до проекту наказу просимо надсилати протягом місяця з дати його оприлюднення на адреси:

- Адміністрації Державної служби спеціального зв'язку та захисту інформації України:

поштова: вул. Солом'янська, 13, м. Київ, 03680; тел. (044) 281-90-10, (044) 281-94-83, факс (044) 226-26-83;

електронна: info@dsszzi.gov.ua;

- Державної регуляторної служби України:

поштова: вул. Арсенальна, 9/11, м. Київ, 01011; тел. (044) 254-56-73, факс (044) 254-43-93;

електронна: inform@dkrp.gov.ua

3. Обраний спосіб оприлюднення проекту акта

Проект акта оприлюднюється в мережі Інтернет: проект наказу та аналіз регуляторного впливу.

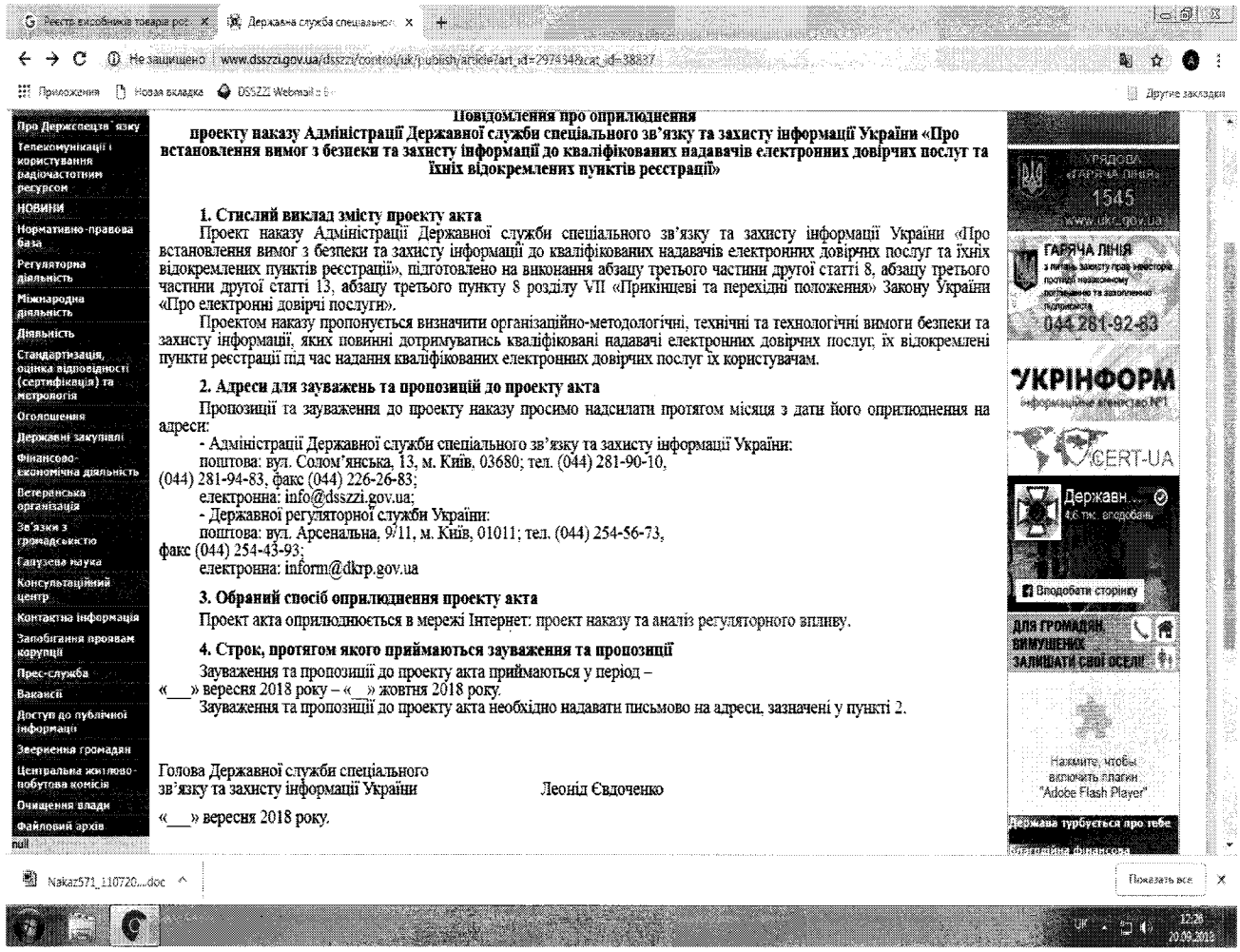
4. Строк, протягом якого приймаються зауваження та пропозиції

Зауваження та пропозиції до проекту акта приймаються у період – «17» вересня 2018 року – «15» жовтня 2018 року.

Зауваження та пропозиції до проекту акта необхідно надавати письмово на адреси, зазначені у пункті 2.

Голова Державної служби спеціального
зв'язку та захисту інформації України Леонід Євдоченко

«17» вересня 2018 року.



Реєстр виробників товарів роз | Державна служба спеціального | www.dsszzi.gov.ua/dsszzi/control/uk/publish/article?art_id=2974349&cat_id=38837

Приложения | Новая вкладка | DSSZZI Webmail :: Б | Другие закладки

Про Держспецзв'язку
Телекомунікації і користування радіочастотним ресурсом
НОВИНИ
Нормативно-правова база
Регуляторна діяльність
Міжнародна діяльність
Діяльність
Стандартизація, оцінка відповідності (сертифікація) та метрологія
Оголошення
Державні закупівлі
Фінансово-економічна діяльність
Ветеранська організація
Зв'язки з громадськістю
Галузева наука
Консультаційний центр
Контактна інформація
Запобігання проявам корупції
Прес-служба
Вакансії
Доступ до публічної інформації
Звернення громадян
Центральна житлово-побутова комісія
Очищення влади
Файловий архів
null

Повідомлення про оприлюднення
проекту наказу Адміністрації Державної служби спеціального зв'язку та захисту інформації України «Про встановлення вимог з безпеки та захисту інформації до кваліфікованих надавачів електронних довірчих послуг та їхніх відокремлених пунктів реєстрації»

1. Стислий виклад змісту проекту акта

Проект наказу Адміністрації Державної служби спеціального зв'язку та захисту інформації України «Про встановлення вимог з безпеки та захисту інформації до кваліфікованих надавачів електронних довірчих послуг та їхніх відокремлених пунктів реєстрації», підготовлено на виконання абзацу третього частини другої статті 8, абзацу третього частини другої статті 13, абзацу третього пункту 8 розділу VII «Прикінцеві та перехідні положення» Закону України «Про електронні довірчі послуги».

Проектом наказу пропонується визначити організаційно-методологічні, технічні та технологічні вимоги безпеки та захисту інформації, яких повинні дотримуватись кваліфіковані надавачі електронних довірчих послуг, їх відокремлені пункти реєстрації під час надання кваліфікованих електронних довірчих послуг їх користувачам.

2. Адреси для зауважень та пропозицій до проекту акта

Пропозиції та зауваження до проекту наказу просимо надсилати протягом місяця з дати його оприлюднення на адреси:

- Адміністрації Державної служби спеціального зв'язку та захисту інформації України:
поштова: вул. Солом'янська, 13, м. Київ, 03680; тел. (044) 281-90-10, (044) 281-94-83, факс (044) 226-26-83;
електронна: info@dsszzi.gov.ua;
- Державної регуляторної служби України:
поштова: вул. Арсенальна, 9/11, м. Київ, 01011; тел. (044) 254-56-73, факс (044) 254-43-93;
електронна: inform@dkrp.gov.ua

3. Обраний спосіб оприлюднення проекту акта

Проект акта оприлюднюється в мережі Інтернет: проект наказу та аналіз регуляторного впливу.

4. Строк, протягом якого приймаються зауваження та пропозиції

Зауваження та пропозиції до проекту акта приймаються у період – «___» вересня 2018 року – «__» жовтня 2018 року.

Зауваження та пропозиції до проекту акта необхідно надавати письмово на адреси, зазначені у пункті 2.

Голова Державної служби спеціального зв'язку та захисту інформації України Леонід Євдоченко

«___» вересня 2018 року.

УРЯДОВА «ГАРЯЧА ЛІНІЯ» 1545 www.ukc.gov.ua
ГАРЯЧА ЛІНІЯ з питань захисту прав інвесторів, протидії незаконному поглинанню та захопленню підприємств 044 281-92-83
УКРІНФОРМ інформаційне агентство №1
CERT-UA
Державн... 4,6 тис. вподобань
Вподобати сторінку
ДЛЯ ГРОМАДЯН, ВИМУШЕНИХ ЗАЛИШАТИ СВОЇ ОСЕЛІ!
Нажмите, чтобы включить плагин "Adobe Flash Player"
Держава турбується про тебе
Міністерство фінансів України

Nakaz571_110720....doc | Показать все

UK 12:28 20.09.2018