Прим. № 1

АДМІНІСТРАЦІЯ ДЕРЖАВНОЇ СЛУЖБИ СПЕЦІАЛЬНОГО ЗВ'ЯЗКУ ТА ЗАХИСТУ ІНФОРМАЦІЇ УКРАЇНИ
(АДМІНІСТРАЦІЯ ДЕРЖСПЕЦЗВ'ЯЗКУ)

вул. Солом'янська, 13, м. Київ, 03110, тел. (044) 281-92-10, факс: (044) 281-94-83,
e-mail: info@dsszzi.gov.ua, сайт: www.dsszzi.gov.ua, код згідно з ЄДРПОУ 34620942

21.08.2019 № 04/04/03-895 На № _____ від _____

Державна регуляторна служба України
вул. Арсенальна, 9/11, м. Київ, 01011

На виконання вимог 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, Адміністрацією Держспецзв'язку підготовано проєкт наказу «Про встановлення вимог з безпеки та захисту інформації до кваліфікованих надавачів електронних довірчих послуг та їхніх відокремлених пунктів реєстрації» (далі – Наказ).

Означений Наказ погоджено без зауважень Державною регуляторною службою України.

У зв'язку зі зміною складу Кабінету Міністрів України та урахуванням зауважень та пропозицій Міністерства цифрової трансформації щодо винесення вимог до спеціальних приміщень з тексту Наказу у рекомендації для публікування на офіційному вебсайті Держспецзв'язку та встановлення відсилочної норми щодо здійснення оцінки ризиків згідно відповідних стандартів, просимо здійснити повторний розгляд та погодження Наказу.

Додатки:
1. Наказ на 10 арк.
2. Пояснювальна записка на 4 арк.
3. Аналіз регуляторного впливу, на 15 арк.
4. Повідомлення про оприлюднення, на 1 арк.
5. Копія листа Державної регуляторної служби України, прим. №__, на 2 арк., вх. від 21.08.2019 № 5069.

Голова Служби Валентин ПЕТРОВ

Микола Сніжинський
281-97-47

ПРОЄКТ

АДМІНІСТРАЦІЯ ДЕРЖАВНОЇ СЛУЖБИ СПЕЦІАЛЬНОГО ЗВ'ЯЗКУ ТА ЗАХИСТУ ІНФОРМАЦІЇ УКРАЇНИ

Н А К А З

м. Київ

___.___.20__ № ____

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,

НАКАЗУЮ:

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

2. 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.

3. Цей наказ набирає чинності з дня його офіційного опублікування.

4. Кваліфікованим надавачам електронних довірчих послуг забезпечити:

1) приведення їх діяльності у відповідність до Вимог шляхом внесення змін до регламентів їх роботи до 07 листопада 2020 року;

2) виконання пунктів 1 та 2 розділу IV Вимог, до закінчення строку чинності атестатів відповідності на комплексну систему захисту інформації інформаційно-телекомунікаційної системи, що застосовується ними для надання кваліфікованих електронних довірчих послуг, але не пізніше 01 січня 2023 року.

5. Контроль за виконанням цього наказу покласти на заступника Голови Державної служби спеціального зв'язку та захисту інформації України відповідно до розподілу функціональних обов'язків.

Голова Служби Валентин ПЕТРОВ

Валентин ПЕТРОВ

ЗАТВЕРДЖЕНО

Наказ Адміністрації Державної служби спеціального зв'язку та захисту інформації України _____ 2020 року № ___

Вимоги

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

І. Загальні положення

1. Положення цих Вимог є обов'язковими для кваліфікованих надавачів електронних довірчих послуг (далі – надавач) під час надання ними послуг користувачам електронних довірчих послуг (далі – користувач), а також для відокремлених пунктів реєстрації (далі – ВПР) під час реєстрації користувачів.

2. Ці Вимоги деталізують та визначають спосіб виконання положень Закону України «Про електронні довірчі послуги» та Вимог у сфері електронних довірчих послуг, затверджених постановою Кабінету Міністрів України від 07 листопада 2018 року № 992, щодо забезпечення безпеки та захисту інформації надавачів та ВПР.

3. Забезпечення безпеки інформації надавача або ВПР здійснюється шляхом комплексного застосування необхідного набору взаємодоповнюючих

заходів щодо захисту інформації в ІТС надавача або ВПР, організаційних (адміністративних) заходів, відповідності приміщень, сховищ, програмно-технічного комплексу та електронних засобів технічним вимогам.

4. Діяльність з безпеки та захисту інформації надавача (ВПР) організовується, постійно підтримується та координується службою захисту інформації (далі – СЗІ) з дотриманням вимог законодавства у сфері захисту інформації, електронних довірчих послуг та регламенту роботи надавача.

5. У цих Вимогах терміни вживаються у таких значеннях:

вразливість – недостатня стійкість активу або заходу нейтралізації протистояти реалізації певній загрозі або сукупності загроз;

загроза – потенційна можливість реалізації вразливості;

критичний компонент – компонент, порушення захисту якого впливає на надання кваліфікованих електронних довірчих послуг;

приміщення – приміщення надавача або ВПР, призначені для розміщення програмно-технічного комплексу (далі – ПТК) або його складових, що використовується під час надання кваліфікованих електронних довірчих послуг та за ступенем обмеження доступу поділяються на рівні безпеки;

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

спеціальне приміщення (зона підвищеної безпеки) – приміщення, призначене для розміщення складових програмно-технічного комплексу з метою генерації, використання, зберігання та резервування особистих ключів надавача;

реєстрація – процедура, в рамках якої забезпечуються встановлення особи користувача, збір, перевірка та внесення до реєстру користувачів ідентифікаційних даних, необхідних для надання кваліфікованої електронної довірчої послуги.

Інші терміни вживаються у значеннях, наведених в Законах України «Про електронні довірчі послуги», «Про захист інформації в інформаційно-телекомунікаційних системах», Правилах забезпечення захисту інформації в інформаційних, телекомунікаційних та інформаційно-телекомунікаційних системах, затверджених постановою Кабінету Міністрів України від 29 березня 2006 року № 373 (далі – Правила), Вимогах у сфері електронних довірчих послуг, затверджених постановою Кабінету Міністрів України від 07 листопада 2018 року № 992.

II. Вимоги із захисту інформації

1. Інформаційно-телекомунікаційні системи (далі – ІТС), що використовуються для цілей, встановлених у пункті 1 розділу I цих Вимог, повинні відповідати вимогам із захисту інформації шляхом впровадження комплексної системи захисту інформації (далі – КСЗІ) або системи управління інформаційною безпекою (далі – СУІБ) з підтвердженою відповідністю з дотриманням вимог законодавства у сфері захисту інформації та цих Вимог, якщо інше не встановлено Законом України «Про захист інформації в інформаційно-телекомунікаційних системах».

2. КСЗІ створюється відповідно до вимог нормативних документів системи технічного захисту інформації, затверджених Адміністрацією Держспецзв'язку.

СУІБ створюється відповідно до вимог стандартів, що визначають вимоги до інформаційної безпеки, визначених Переліком стандартів, що застосовуються кваліфікованими надавачами електронних довірчих послуг під час надання кваліфікованих електронних довірчих послуг, що додається до Вимог у сфері електронних довірчих послуг, затверджених постановою Кабінету Міністрів України від 07 листопада 2018 року № 992.

3. Підтвердження відповідності КСЗІ здійснюється відповідно до вимог Положення про державну експертизу в сфері технічного захисту інформації,

затвердженого наказом Адміністрації Держспецзв'язку від 16 травня 2007 року № 93, зареєстрованого в Міністерстві юстиції України 16 липня 2007 року за № 820/14087 (із змінами).

Підтвердження відповідності СУІБ здійснюється відповідно до Порядку проведення процедури оцінки відповідності у сфері електронних довірчих послуг, затвердженого постановою Кабінету Міністрів України від 18 грудня 2018 року № 1215.

4. У випадку віднесення відповідно до законодавства у сфері кіберзахисту кваліфікованого надавача електронних довірчих послуг до об'єкта критичної інфраструктури в ІТС надавача повинні бути впровадженні заходи з кіберзахисту відповідно до вимог постанови Кабінету Міністрів України від 19 червня 2019 року № 518 «Про затвердження Загальних вимог до кіберзахисту об'єктів критичної інфраструктури».

5. Надання кваліфікованих електронних довірчих послуг та здійснення реєстрації користувачів без чинних документів, що підтверджують відповідність ІТС вимогам законодавства у сфері захисту інформації, забороняються.

ІІІ. Організаційні вимоги

1. У регламенті роботи надавача в положеннях політики сертифіката та/або в положеннях з опису процедур і процесів, які виконуються під час надання кваліфікованих електронних довірчих послуг, що не передбачають формування та обслуговування кваліфікованих сертифікатів відкритих ключів, повинно бути визначено необхідність встановлення вимог до процедур з управління ризиками, персоналом, операційною безпекою, інцидентами, доказами та архівами, поводження з персональними даними користувачів, процедур встановлення заявника, ВПР та виїзних адміністраторів реєстрації, опису фізичного середовища з урахуванням цих Вимог та елементів технічних специфікацій та процедур для високого рівня довіри до засобів електронної

ідентифікації, встановлених Вимогами до засобів електронної ідентифікації, рівнів довіри до засобів електронної ідентифікації для їх використання у сфері електронного урядування, затвердженими наказом Державного агентства з питань електронного урядування від 27 листопада 2018 року № 86, зареєстрованими Міністерством юстиції України 26 грудня 2018 року за № 1462/32914.

2. Надавач повинен захищати свої активи відповідно до проведеної оцінки ризиків. Процедури з управління ризиками повинні передбачати виконання заходів з оцінки ризиків з урахуванням цих Вимог.

3. Процедури з управління персоналом повинні передбачати:

1) наявність у надавача щонайменше двох посад адміністратора безпеки та аудиту;

2) щорічне проходження адміністратором безпеки та аудиту практичних навчань з інформаційної безпеки, що передбачають вивчення нових загроз інформаційної безпеки та реагування на них;

3) заборону суміщення посадових обов'язків адміністратора безпеки та аудиту з іншими посадовими обов'язками, безпосередньо пов'язаними з наданням кваліфікованих електронних довірчих послуг;

4) встановлення відповідних вимог щодо кваліфікації персоналу, безпосередньо пов'язаного з наданням кваліфікованих електронних довірчих послуг.

4. Процедури з управління операційною безпекою

4.1. Процедури з управління операційною безпекою повинні передбачати:

1) контроль використання носіїв інформації в ІТС, спрямований запобіганню їх викраденню, пошкодженню, використанню понад експлуатаційного терміну, несанкціонованому доступу та використанню;

2) контроль встановлення оновлення комп'ютерних програм та оновлень безпеки;

3) резервне копіювання даних, необхідних для функціонування ІТС, у територіально відокремлених місцях із забезпеченням захисту цих даних від модифікації та несанкціонованого ознайомлення;

4) режим доступу до службових та спеціальних приміщень.

4.2. Забороняється застосування оновлень безпеки, які містять уразливості та є нестабільними. Причини невикористання оновлень безпеки документуються.

4.3. Забороняється оновлення комп'ютерних програм, що застосовуються в ІТС, з неідентифікованих та неавтентифікованих джерел.

5. Процедури з управління інцидентами повинні передбачати:

1) виконання заходів, визначених Порядком координації діяльності органів державної влади, органів місцевого самоврядування, військових формувань, підприємств, установ і організацій незалежно від форм власності з питань запобігання, виявлення та усунення наслідків несанкціонованих дій щодо державних інформаційних ресурсів в інформаційних, телекомунікаційних та інформаційно-телекомунікаційних системах, затвердженим наказом Адміністрації Держспецзв'язку від 10 червня 2008 року № 94, зареєстрованим в Міністерстві юстиції України 07 липня 2008 року за № 603/15294;

2) інформування контролюючого органу про порушення вимог з безпеки та захисту інформації, визначені в абзаці одинадцятому частини другої статті 13 Закону України «Про електронні довірчі послуги», протягом 24 годин після виявлення порушення;

3) інформування користувачів, яким надаються послуги, про порушення безпеки, які спричиняють на них негативний вплив, протягом двох годин після виявлення порушення.

6. Процедури з управління доказами та архівами

6.1. Процедури з управління доказами та архівами повинні передбачати ведення журналів аудиту подій, у яких реєструються події таких типів:

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

2) заміна 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.

6.2. Усі записи в журналах аудиту подій в електронній або паперовій формі повинні містити дату та час події, а також ідентифікувати суб'єкта, що її ініціював або брав у ній участь.

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

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

6.5. Журнали аудиту подій повинні бути захищені від неавторизованого перегляду, модифікації і знищення.

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

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

7. Вимоги до поводження з персональними даними користувачів

7.1. Справи підписувачів зберігаються у приміщеннях та сховищах із забезпеченням розмежування доступу персоналу надавача або ВПР відповідно до посадових обов'язків.

7.2. Дозволяється тимчасове зберігання (протягом робочого дня) справ підписувачів у місці їх реєстрації у разі забезпечення їх захисту від несанкціонованого доступу (зберігання зачиненими у вогнестійкій шафі, сейфі).

7.3. У разі реалізації механізмів автентифікації підписувачів за ключовою фразою дані фраз ключової автентифікації повинні зберігатися в ІТС надавача із забезпеченням доступу до такої інформації виключно персоналу надавача, відповідального за управління статусами сертифікатів відкритих ключів підписувачів.

8. Вимоги до процедур встановлення заявника, ВПР та виїзних адміністраторів реєстрації

8.1. Процедури встановлення особи-заявника повинні використовувати наявні сервіси перевірки чинності документів та ідентифікаційної інформації про особу. До таких сервісів можуть належати сервіси «Перевірка за базою недійсних документів» (nd.dmsu.gov.ua) та «Єдиний державний реєстр юридичних осіб, фізичних осіб-підприємців та громадянсьих формувань» (usr.minjust.gov.ua).

8.2. Верифікація даних ID-картки здійснюється одним із таких способів:

без залучення додаткових пристроїв шляхом візуального зіставлення однакової інформації (значення «УНЗР», «документ №», «дата народження», «строк дії»), яка надрукована в зоні візуальної перевірки та машинозчитувальній зоні;

шляхом автоматизованого зчитування інформації з використанням апаратних та програмних засобів (зчитувачів), які мають інтерфейс, опублікований на офіційному вебсайті державного підприємства «Поліграфічний комбінат «Україна».

8.3 Якщо надавач має намір надавати кваліфіковані електронні довірчі послуги через ВПР або застосовувати процедури виїзної реєстрації, у регламенті роботи надавача в положеннях політики сертифіката визначаються вимоги до публікації на офіційному вебсайті надавача ідентифікаційних даних

про ВПР та виїзних адміністраторів реєстрації в обсязі, достатньому для однозначного їх встановлення заявником.

IV. Технічні вимоги

1. Вимоги до приміщень надавача

1.1. Приміщення надавача повинні бути розділені на функціональні зони за рівнями безпеки приміщень, встановленими надавачем.

Для кожного рівня безпеки приміщень визначаються мінімально необхідний набір механізмів безпеки, зокрема: контролю доступу, виявлення вторгнень, пожежної сигналізації та пожежогасіння, альтернативних та резервних джерел електроживлення тощо (далі – механізми безпеки приміщень).

Механізми безпеки приміщень можуть бути змінені на підставі оцінених ризиків та відповідних цим ризикам обраних механізмів їх нейтралізації.

Рекомендації до встановлення рівнів безпеки та механізмів безпеки приміщень, застосування яких забезпечує ці рівні, публікуються Адміністрацією Державної служби спеціального зв'язку та захисту інформації України на офіційному вебсайті.

1.2. Компоненти, які є критичними для безпечної роботи надавача, мають розташовуватися в захищеному та безпечному середовищі з фізичним захистом від вторгнення, контролем доступу через периметр безпеки та сигналізацією для виявлення вторгнення.

2. Вимоги до безпечного сховища

2.1. Безпечне сховище, що знаходиться у спеціальному приміщенні, призначене для зберігання носіїв виключно критичної для надання послуг надавачем інформації (атрибути доступу до засобів кваліфікованого електронного підпису чи печатки, в яких зберігаються дані резервних копій особистого ключа надавача, засоби авторизації в ПТК надавача тощо).

2.2. Конструкція сховища повинна передбачати достатню кількість індивідуальних відсіків для кожної уповноваженої посадової особи, яка згідно з посадовими обов'язками виконує роботи з критичною для надавача інформацією.

2.3. Доступ до відсіків здійснюється за участі двох уповноважених посадових осіб, які згідно з посадовими обов'язками виконують роботи з критичною для надавача інформацією.

2.4. Безпечне сховище повинно мати сертифікат про відповідність ДСТУ EN 1143-1 «Засоби безпечного зберігання. Вимоги, класифікація та методи випробування на тривкість щодо зламування. Частина 1: Сховища, двері сховищ, сейфи та АТМ-сейфи».

3. Вимоги до ПТК

ПТК, що використовується під час надання електронних довірчих послуг, повинен відповідати вимогам наказу Міністерства юстиції України, Адміністрації Державної служби спеціального зв'язку та захисту інформації України від 18 листопада 2019 року № 3563/5/610 «Про встановлення вимог до технічних засобів, процесів їх створення, використання та функціонування у складі інформаційно-телекомунікаційних систем під час надання електронних довірчих послуг», зареєстрованого в Міністерстві юстиції України 20 листопада 2019 року за № 1172/34143.

V. Вимоги до оцінки ризиків

1. Оцінка ризиків

Оцінка ризиків здійснюється на основі вимог ДСТУ ISO/IEC 27005:2015 (ISO/IEC 27005:2011, IDT) "Інформаційні технології. Методи захисту. Управління ризиками інформаційної безпеки" та інших нормативних документів з оцінки ризиків.

Для здійснення оцінки ризиків надавачем вживаються заходи щонайменше передбачені цим розділом.

1.1. Процедури оцінки ризиків повинні містити заходи з визначення активів, загроз, вразливостей, ймовірності реалізації загроз та оцінки їх

наслідків, заходи з нейтралізації. Значення ризиків є відносною величиною, яка дозволяє оцінювати їх вплив на діяльність надавача.

1.2. Ризики оцінюються за такою формулою:

РИЗИК = ВРАЗЛИВІСТЬ * НАСЛІДКИ РЕАЛІЗАЦІЇ ЗАГРОЗ

де:

«вразливість» має значення від 0 до 2 та обчислюється відповідно до пункту 4 розділу V цих Вимог;

«наслідки реалізації загроз» мають значення від 1 до 5 та обчислюються відповідно до пункту 3 розділу V цих Вимог;

«*» є математичною операцією множення.

1.3. Ризики, які приймають значення більше/рівно 4, вважаються неприйнятними та потребують обов'язкового вжиття заходів щодо їх нейтралізації.

2. Визначення активів

2.1. До активів надавача належать матеріальні об'єкти, які надавач може оцінити з точки зору їх вартості, інформація, яку надавач збирає та/або формує і зберігає із забезпеченням належного рівня довіри, а також відповідні процеси.

2.2. Усі активи повинні бути ідентифіковані та задекларовані. Для кожного активу призначаються особи, відповідальні за його захист і підтримку.

2.3. Після ідентифікації активів проводиться оцінка їх цінності для надавача. Цінність активу визначається на основі оцінки негативних наслідків можливого інциденту, який впливає на нього. Цінність активу може мати якісні (критичність) і кількісні (вартість) характеристики.

2.4. Активи повинні бути класифіковані на підставі їхнього типу та характеристик та належати до таких категорій:

1) основні активи, які містять інформаційні активи та процеси;

2) активи підтримки, які містять програмно-апаратні засоби, обладнання, мережу, персонал та місця розташування тощо.

2.5. До основних активів щонайменше повинні належати такі:

1) інформаційні активи:

особисті ключі надавача;

сертифікати відкритих ключів надавача;

реєстраційні дані заявників;

сертифікати відкритих ключів користувачів;

запити на зміну статусу сертифіката;

списки відкликаних сертифікатів;

журнали аудиту;

архіви;

2) активи процесів:

генерація пар ключів надавача;

використання, резервне копіювання та відновлення ключів надавача;

знищення особистих ключів надавача;

формування сертифікатів відкритих ключів;

розповсюдження сертифікатів відкритих ключів;

управління статусом сертифікатів відкритих ключів;

реєстрація заявників;

функціонування інтегрованої електронної системи безпеки, що забезпечує безперебійну експлуатацію об'єктів і критичних систем надавача в середовищі із загальним високим рівнем безпеки(далі – ЕСБ).

2.6. До активів підтримки щонайменше повинні належати такі:

1) програмне забезпечення та обладнання ІТС надавача та ВПР:

апаратне забезпечення, на якому базується ПТК надавача;

програмне забезпечення, що використовується в складі ПТК;

апаратне забезпечення ВПР;

програмне забезпечення ВПР;

USB носії та захищені носії інформації, які використовуються в ПТК та ВПР, смарт-карти тощо;

мережева інфраструктура;

обладнання ЕСБ;

обладнання для забезпечення безперебійного електроживлення;

2) активи розміщення:

спеціальне та службові приміщення надавача;

приміщення ВПР;

середовище розміщення вебсайту надавача;

3) активи персоналу:

працівники надавача, посадові обов'язки яких безпосередньо пов'язані з наданням кваліфікованих електронних довірчих послуг;

працівники надавача, що забезпечують виконання функцій, які не пов'язані безпосередньо з наданням кваліфікованих електронних довірчих послуг;

4) загальні активи:

ділова репутація надавача;

дотримання законодавства;

довірчі відносини надавача (відносини з діловими партнерами, постачальниками електроенергії та телекомунікаційних послуг, контролюючими органами, компаніями, що займаються обслуговуванням та оновленням засобів ПТК, мережі тощо);

клієнтська база надавача.

3. Визначення загроз

3.1. Процедури визначення загроз повинні передбачати заходи з виявлення загроз, оцінки ймовірності їх виникнення та наслідків. Загрози визначаються для кожного з визначених активів.

3.2. Надавач повинен сформувати перелік потенційних загроз з оцінкою ймовірності їх виникнення, який відповідає його реальному діловому та операційному середовищу.

Ймовірність виникнення кожної загрози оцінюється на основі:

мотивації суб'єкта загрози за кожною загрозою;

можливості реалізації вразливості з урахуванням існуючих контрзаходів;

аналізу минулих подій.

Щодо кожної загрози оцінюються наслідки її реалізації диференційно за шкалою від 1 до 5.

Значення 1 приймається, коли немає наслідків для діяльності надавача.

Значення 5 приймається, коли є критичні наслідки, які можуть призвести до припинення діяльності надавача.

3.3. За характером виникнення загрози можуть поділятися на природні, антропогенні, загрози неотримання надавачем необхідних засобів чи сервісів, за місцем виникнення – на внутрішні або зовнішні, бути випадковими або навмисними. Цей перелік загроз не є вичерпним. Загроза належить до певної категорії за її переважаючими характеристиками.

3.4. Природні загрози та ймовірність їх виникнення визначаються з урахуванням фізичного розташування інфраструктури надавача та статистичного аналізу попередніх подій. До природніх загроз можуть належати:

сейсмічні або гідрологічні події;

пожежі;

пошкодження водою (затоплення) або корозія;

електромагнітні явища (аномалії);

буревії.

3.5. Загрози неотримання надавачем необхідних засобів чи сервісів визначаються на основі аналізу операцій надавача, проведення яких потребує періодичного чи систематичного отримання певних засобів чи сервісів, а їх неотримання може призвести до зупинки діяльності надавача або його підрозділів. До загроз неотримання надавачем необхідних засобів чи сервісів можуть належати:

електропостачання;

доступ до телекомунікаційних мереж;

обслуговування систем охолодження;

необхідне для роботи обладнання та/або витратні матеріали.

3.6. Антропогенні загрози (обумовлені діями людини) визначаються на основі аналізу операцій надавача, у виконанні яких бере участь людина. Антропогенні загрози поділяються на навмисні (викликані суб'єктами загроз) або випадкові.

До антропогенних загроз можуть належати:

крадіжка або втрата обладнання та/або даних;

випадкове знищення обладнання та/або даних;

несанкціонований доступ до обладнання та даних;

шкідливе програмне забезпечення;

витік інформації;

криптоаналіз.

До суб'єктів загроз можуть належати:

зловмисники;

комп'ютерні злочинці;

шпигунські організації;

невдоволені працівники.

У певних випадках природні загрози і загрози неотримання надавачем необхідних засобів чи сервісів також можуть бути викликані суб'єктом загрози (бути навмисними).

4. Визначення вразливостей

4.1. Можливі вразливості визначаються для встановлення потенційної слабкості активу або групи активів до загроз. Для визначення потенціалу вразливості застосовуються визначені активи, загрози, заходи нейтралізації загроз. При визначенні потенційних вразливостей оцінюються усі активи надавача.

4.2. Вразливість активу визначається за такою формулою:

ВРАЗЛИВІТЬ = ЗАГРОЗА / (ЗАХОДИ НЕЙТРАЛІЗАЦІЇ ЗАГРОЗИ+АКТИВ)

де:

«загроза» має значення 0 за її відсутності, 1 при низькій ймовірності або 2 за її наявності;

«заходи нейтралізації загрози» мають значення 0 за відсутності гарантій щодо їх ефективної протидії реалізації загроз щодо певного активу або 2, якщо вони здатні ефективно протидіяти реалізації загроз щодо певного активу;

«актив» має значення 1;

«/» є математичною операцією ділення;

«+» є математичною операцією додавання.

4.3. Якщо вразливість приймає значення більше або рівне 1, необхідне запровадження додаткових заходів нейтралізації. Якщо вразливість приймає значення менше за 1, вона вважається нейтралізованою або відсутньою (значення 0).

4.4. Надавач проводить заходи нейтралізації загроз шляхом виконання вимог законодавства у сфері електронних довірчих послуг та вживає інших адекватних заходів відповідно до вимог стандартів у сфері інформаційної безпеки.

До заходів нейтралізації належать ті заходи, що здатні ефективно протидіяти реалізації загрози щодо певного активу.

Одна загроза може бути застосована щодо одного або кількох активів.

Один захід нейтралізації може бути застосований щодо однієї або кількох загроз.

4.5. При визначенні потенційних вразливостей оцінюються щонайменше такі процеси:

реєстрація заявників, подій, ведення журналів аудиту та архівів;

управління ключами надавача (генерація, резервне копіювання, відновлення, зберігання, використання та знищення);

використання засобів кваліфікованого електронного підпису;

механізми перевірки факту володіння заявником особистим ключем та отримання від заявника відкритого ключа;

автентифікація користувачів при поданні запитів на зміну статусу сертифіката;

забезпечення діяльності надавача (отримання надавачем послуг забезпечення електропостачанням, зв'язком, розхідними матеріалами та обладнанням тощо).

4.6. До вразливостей процесів реєстрації заявників, подій, ведення журналів аудиту та архівів можуть належати:

неадекватність або відсутність політик підтвердження ідентичності, що може призвести неправильної ідентифікації суб'єкта-заявника;

неадекватність або відсутність політик ведення та зберігання журналів аудиту;

недостатній захист ВПР від шкідливого програмного забезпечення, що може здійснювати несанкціоновані запити на сертифікацію або призвести до несправності ПТК;

недостатній рівень захисту реєстраційних записів та архівів.

4.7. До вразливостей процесів керування ключами можуть належати:

відсутність резервного копіювання особистих ключів надавача;

недостатній захист резервних копій особистих ключів надавача;

невикористання засобів і заходів, які гарантують неможливість відновлення особистого ключа надавача при його знищенні.

4.8. До вразливостей процесів використання засобів кваліфікованого електронного підпису можуть належати:

неадекватність або відсутність політик перевірки застосування користувачами засобів кваліфікованого електронного підпису для генерації особистих ключів та їх зберігання;

використання для зберігання особистих ключів засобів кваліфікованого електронного підпису, які не забезпечують захист особистих ключів від

несанкціонованого доступу, від безпосереднього ознайомлення зі значенням параметрів особистих ключів та їх копіювання.

4.9. До вразливостей механізмів перевірки факту володіння заявником особистим ключем та отримання від заявника відкритого ключа можуть належати:

неадекватність або відсутність політик перевірки володіння заявником особистим ключем;

відсутність перевірки на наявність шкідливого програмного забезпечення носіїв інформації, на яких заявники подають до надавача попередньо сформовані запити на сертифікацію з відкритими ключами, та/або підключення таких носіїв безпосередньо до ПТК надавача.

4.10. До вразливостей процесів автентифікації користувачів при поданні ними запитів на зміну статусу сертифіката може належати неадекватність або відсутність політик автентифікації користувачів за ключовою фразою.

4.11. До вразливостей процесів забезпечення діяльності надавача можуть належати:

укладання з постачальником електроенергії договору, який не гарантує усунення перебоїв електропостачання протягом часу можливого забезпечення безперебійного електроживлення системою автономного електроживлення;

відсутність резервування телекомунікаційних мереж доступу;

відсутність обліку та завчасного замовлення витратних матеріалів, необхідних для роботи надавача;

експлуатація техніки та обладнання понад встановлені експлуатаційні терміни.

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

ПОЯСНЮВАЛЬНА ЗАПИСКА

до проєкту 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. Резюме

Метою прийняття проєкту наказу є 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.

2. Проблема, яка потребує розв'язання

Необхідність прийняття проєкту 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 проєкту 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, 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 проєкту акта

Проєктом наказу пропонується визначити організаційно-методологічні, технічні та технологічні вимоги безпеки та захисту інформації, яких повинні дотримуватися 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 упровадження 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 проєкту наказу.

4. Вплив на бюджет

Виходячи з проведеної фінансово-економічної оцінки, реалізація проєкту 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 надавачів електронних довірчих послуг.

На сьогодні в Україні функціонують 24 кваліфіковані надавачі електронних довірчих послуг, з яких 6 фінансуються за рахунок державного бюджету.

Вартість реалізації одним надавачем електронних довірчих послуг (державного органу або суб'єкта господарювання) заходів, передбачених проєктом наказу (з урахуванням заходів державного нагляду (контролю), у 2020 році щонайменше складатиме 356 600,00 грн. (зведені фінансово-економічні розрахунки до проєкту наказу наведено в аналізі регуляторного впливу, опублікованому на офіційному вебсайті Держспецзв'язку у розділі «Регуляторна діяльність»).

5. Позиція заінтересованих сторін

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

Прогноз впливу реалізації акта на ключові інтереси заінтересованих сторін наведено в аналізі регуляторного впливу, опублікованому на офіційному вебсайті Держспецзв'язку у розділі «Регуляторна діяльність».

За предметом правового регулювання проєкт 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.

З метою проведення громадського обговорення проєкт наказу розміщено на офіційному вебсайті Держспецзв'язку.

6. Прогноз впливу

Реалізація наказу впливатиме 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 проєкту наказу.

Реалізація проєкту 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 проєкт наказу не матиме впливу на:

розвиток регіонів;

громадське здоров'я;

екологію та навколишнє природне середовище.

7. Позиція заінтересованих органів

Проєкт наказу погоджено без зауважень з Антимонопольним комітетом України, Міністерством фінансів України, Державним агентством з питань електронного урядування України, Державною регуляторною службою України, потребує додаткового погодження з Міністерством цифрової трансформації України. Міністерство економічного розвитку і торгівлі України поінформувало, що проєкт наказу не потребує в установленій законодавством формі погодження з означеним органом влади.

8. Ризики та обмеження

У проєкті наказу немає положень, які містять ознаки дискримінації.

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

У проєкті наказу немає правил і процедур, які можуть містити ризики вчинення корупційних правопорушень.

Проєкт наказу не потребує проведення громадської антикорупційної та/або антидискримінаційної експертизи.

9. Підстава розроблення проєкту акта

Правовими підставами розроблення проєкту наказу є положення:

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.

Голова Державної служби спеціального зв'язку та захисту інформації України Валентин ПЕТРОВ

«___» _____ 2020 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».

Проект наказу поширюватиметься на суб'єктів господарювання, що надають кваліфіковані електронні довірчі послуги, відомості про яких внесено до Довірчого списку (czo.gov.ua/trustedlist) на підставі рішення центрального засвідчувального органу або засвідчувального центру (у разі надання електронних довірчих послуг у банківській системі України та при здійсненні переказу коштів).

Необхідність прийняття проекту наказу полягає у потребі врегулювання питань забезпечення належного рівня безпеки та захисту інформації при наданні кваліфікованих електронних довірчих послуг.

Проектом наказу передбачено затвердження Вимог з безпеки та захисту інформації до кваліфікованих надавачів електронних довірчих послуг та їхніх відокремлених пунктів реєстрації (далі – Вимоги з безпеки), якими деталізується та визначається спосіб виконання положень Закону України «Про електронні довірчі послуги» та Вимог у сфері електронних довірчих послуг, затверджених постановою Кабінету Міністрів України від 7 листопада 2018 року № 992 (далі – Постанова № 992), щодо забезпечення безпеки та захисту інформації кваліфікованих надавачів електронних довірчих послуг (далі – надавач) та відокремлених пунктів реєстрації (далі – ВПР).

Проектом наказу передбачено забезпечення безпеки інформації надавача або ВПР шляхом комплексного застосування необхідного набору взаємодоповнюючих заходів щодо захисту інформації в ІТС надавача або ВПР, організаційних (адміністративних) заходів, виконання яких повинно бути передбачено Регламентом роботи надавача, відповідності приміщень, сховищ, програмно-технічного-комплексу та електронних засобів технічним вимогам, встановлених Вимогами з безпеки.

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 виконання вимог Закону України «Про електронні довірчі послуги» та Постанови № 992, щодо застосування норм європейських та міжнародних стандартів та кращих європейських практик під час надання кваліфікованих 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 вимог Закону України «Про електронні довірчі послуги» та Постанови № 992 з питань безпеки та захисту інформації без деталізації способу їх виконання. 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;	Прийняття проекту наказу: потребуватиме збільшення видатків з державного бюджету внаслідок запровадження додаткових організаційно-методологічних, технічних та технологічних умов діяльності кваліфікованих

	підвищення рівня довіри до кваліфікованих електронних довірчих послуг.	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.

Оцінка впливу на сферу інтересів громадян:

Вид альтернативи	Вигоди	Витрати
Альтернатива 1 Прийняття	Прийняття проекту наказу матиме такий вплив на	Прийняття проекту наказу може призвести до

проекту наказу	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.	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.
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.

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 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	Прийняття проекту наказу призведе до збільшення витрат суб'єкта 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**	**145 700,00**	**160 700,00**

	обслуговування, навчання / підвищення кваліфікації персоналу тощо, гривень:		
1.1.	проведення модернізації комплексної системи захисту інформації в інформаційно-телекомунікаційній системі кваліфікованого надавача електронних довірчих послуг (придбання обладнання, приладів та ліцензійного програмного забезпечення)	130 700,00	130 700,00
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-	162 600,00	162 600,00

	телекомунікаційної системи кваліфікованого надавача електронних довірчих послуг		
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:**	**56 700,00**	**283 400,00**
6.1.	найм кваліфікованим надавачем електронних довірчих послуг додаткового 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 2020 року – 3723,00 гривні)	56 700,00	283 400,00
7	**РАЗОМ (сума рядків: 1 + 2 + 3 + 4 + 5 + 6), гривень**	**368 600,00**	**617 500,00**

Сумарні витрати за альтернативами	Сума витрат, гривень
Альтернатива 1 Прийняття проекту наказу	368 600,00
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 невиконання рішення Уряду

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	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	Цілі, визначені стратегічним документами досягнуті

	кваліфікованих електронних довірчих послуг; збільшенню прибутку суб'єкта господарювання.	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, 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 цифрової трансформації 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 цифрової трансформації України	1 робочий день	400,00 грн за робочий день (з розрахунку 9 000,00 грн за місяць)	1	24	400,00
5. Оскарження одного окремого рішення суб'єктами господарювання	**2 робочі дні**	**400,00 грн за робочий день (з розрахунку 9 000,00 грн за місяць)**	**2**	**24**	**800,00**
Адміністрація Державної служби спеціального зв'язку та захисту інформації України	1 робочий день	400,00 грн за робочий день (з розрахунку 9 000,00 грн за місяць)	1	24	400,00
Міністерство цифрової трансформації 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 цифрової трансформації України	1 200,00	6 000,00

VII. Обґрунтування 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 дня його офіційного опублікування.

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 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 **Валентин ПЕТРОВ**

«___» _____ 2020 року

Повідомлення про оприлюднення
проєкту 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 проєкту акта

Проєкт 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».

Проєктом 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 проєкту акта

Адміністрації Державної служби спеціального зв'язку та захисту інформації України:
поштова: вул. Солом'янська, 13, м. Київ, 03680;
електронна: info@dsszzi.gov.ua;

Державної регуляторної служби України:
поштова: вул. Арсенальна, 9/11, м. Київ, 01011;
електронна: inform@dkrp.gov.ua.

2. Обраний спосіб оприлюднення проєкту акта

Проєкт акта та аналіз регуляторного впливу розміщено на вебсайті Держспецзв'язку.

3. Строк, протягом якого приймаються зауваження та пропозиції

Пропозиції та зауваження до проєкту акта просимо надсилати протягом місяця з дати його оприлюднення.

Голова Державної служби спеціального зв'язку та захисту інформації України Валентин ПЕТРОВ

«___» _____ 2020 р.

ДЕРЖАВНА РЕГУЛЯТОРНА СЛУЖБА УКРАЇНИ

вул. Арсенальна, 9/11 м. Київ 01011, тел. (044) 254-56-73, факс (044) 254-43-93
E-mail: inform@dkrp.gov.ua, Web: http://www.drs.gov.ua, код ЄДРПОУ 39582357

від _____ №_____

на №_____від_____

РІШЕННЯ
про погодження проекту регуляторного акта

Державна регуляторна служба України відповідно до Закону України «Про засади державної регуляторної політики у сфері господарської діяльності» розглянула 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), а також документи, що додаються до проекту наказу, подані листом Державної служби спеціального зв'язку та захисту інформації України від 05.07.2019 № 04/02/03-1816.

За результатами проведеного аналізу проекту наказу та його аналізу регуляторного впливу на відповідність вимогам статей 4, 5, 8 і 9 Закону України «Про засади державної регуляторної політики у сфері господарської діяльності» та керуючись частиною 4 статті 21 цього Закону, Державна регуляторна служба України

вирішила:

погодити 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».

Голова **К. ЛЯПІНА**

Служба діловодства Адміністрації Держспецзв'язку
Вх. № 2649-Ц
(архів) від 19.08.2019

1
1 5069
21 08 19

Кривошей О.В. 2545825

РІШЕННЯ № 367 від 13.08.2019

Кривошей Олена Володимирівна

Держспецзв'язку
Вх. № 2649-Ц
від 19.08.2019

АРКУШ ПОГОДЖЕННЯ

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»

ПОГОДЖЕНО:

Голова Державної регуляторної служби України **К. ЛЯПІНА**

"_____" _____2019 р.

до вх 5069-19 до вх 2649-18