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

05.07.2019 № 04/02/03-1816

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

На № 10396/0/20-18 від 25.10.2018
Про погодження проекту наказу
Адміністрації Держспецзв'язку

Надсилаємо на повторне 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», підготовлений 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» з урахуванням зауважень та пропозицій заінтересованих суб'єктів до його попередньої редакції.

Просимо розглянути та погодити проект наказу до 19 липня 2019 року.

Додатки: 1. Проект наказу на 26 арк.
2. Пояснювальна записка до проекту наказу на 7 арк.
3. Аналіз регуляторного впливу проекту наказу на 14 арк.
4. Повідомлення про оприлюднення на 1 арк.

Голова Служби Л.О. Євдоченко

Вик. Сніжинський М.М.
Тел. 281-97-47

ПРОЕКТ

АДМІНІСТРАЦІЯ ДЕРЖАВНОЇ СЛУЖБИ СПЕЦІАЛЬНОГО ЗВ'ЯЗКУ ТА ЗАХИСТУ ІНФОРМАЦІЇ УКРАЇНИ

Н А К А З

м. Київ

____.__.2019 № ____

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, 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 опублікування.

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

Голова Служби Л.О. Євдоченко

«_____ Л.О. Євдоченко»

ЗАТВЕРДЖЕНО

Наказ Адміністрації Державної служби спеціального зв'язку та захисту інформації України _____ 2019 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 послуг користувачам електронних довірчих послуг (далі – користувач) та 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 7 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.

СЗІ надавача (ВПР) очолює посадова особа надавача (ВПР) зі складу його керівництва.

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 чотири рівні безпеки;

службові приміщення (безпечна зона) – приміщення рівнів безпеки 2 та 3, доступ в які забезпечується із застосуванням організаційно-технічних заходів контролю (фізичний та логічний контроль);

спеціальне приміщення (зона підвищеної безпеки) – приміщення рівня безпеки 4, призначене для генерації, використання, зберігання та резервування особистих ключів надавача.

реєстрація – процедура в рамках якої забезпечується 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», Правил 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. Створення КСЗІ здійснюється відповідно до вимог нормативних документів системи технічного захисту інформації, затверджених Адміністрацією Держспецзв'язку.

Створення СУІБ здійснюється 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 впроваджені 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, забороняється.

III. Організаційні вимоги

1. В регламенті роботи надавача в положеннях політики сертифіката та/або в положеннях з опису процедур та процесів, які виконуються під час надання кваліфікованих електронних довірчих послуг, що не передбачають формування та обслуговування кваліфікованих сертифікатів відкритих ключів, визначаються вимоги 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, затверджених наказом Державного агентства з питань електронного урядування від 27 листопада 2018 року № 86, зареєстрованого 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 включати 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 включають 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 включати:

1) контроль використання носіїв інформації в ІТС, спрямований запобіганню їх викраденню, пошкодженню, використанню понад експлуатаційного терміну, несанкціонованого 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 включати:

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, затвердженого наказом Адміністрації Держспецзв'язку від 10 червня 2008 року № 94, зареєстрованого в Міністерстві юстиції України 07 липня 2008 року за № 603/15294;

2) інформування контролюючого органу про порушення вимог з безпеки та захисту інформації, встановленні у 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 включати ведення журналів аудиту подій в 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 здійснив або ініціював.

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 захищенні від неавторизованого перегляду, модифікації і знищення.

6.6. Записи подій у журналах аудиту подій в 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 в вогнестійкій шафі, сейфі).

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

7.4. У разі надання послуг особам-резидентам Європейського Союзу надавач та/або ВПР бере на себе зобов'язання забезпечувати захист персональних даних відповідно до вимог статті 24 Регламенту Європейського Парламенту і Ради (ЄС) 2016/679 від 27 квітня 2016 року про захист фізичних

осіб у зв'язку з опрацюванням персональних даних і про вільний рух таких даних, та про скасування Директиви 95/46/СС (Загальний регламент про захист даних).

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 може бути віднесено сервіс «Перевірка за базою недійсних документів» (nd.dmsu.gov.ua), сервіс «Єдиний державний реєстр юридичних осіб, фізичних осіб-підприємців та громадянських формувань» (usr.minjust.gov.ua).

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

без залучення додаткових пристроїв шляхом візуального співставлення 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 веб-сайті державного підприємства «Поліграфічний комбінат «Україна».

8.3. У разі 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 веб-сайті 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, встановленими цими Вимогами.

У рівнях безпеки визначаються механізми контролю доступу, виявлення вторгнень, пожежної сигналізації та пожежогасіння, альтернативних та резервних джерел електроживлення тощо (далі – механізми безпеки).

Приклад схематичного зображення рівнів безпеки та механізмів безпеки наведено у додатку 1 до цих Вимог.

1.2. Комплексне застосування механізмів безпеки має забезпечувати інтегровану взаємно доповнюючу електронну систему безпеки (далі – ЕСБ), що забезпечує безперебійну експлуатацію об'єктів і критичних систем надавача в середовищі з загальним високим рівнем безпеки.

До складу ЕСБ повинні входити щонайменше такі підсистеми:

контролю доступу (далі – КД);

виявлення вторгнень та сигналізації (далі – ВВС);

відеоспостереження замкнутого контуру (далі – ВСК);

автоматичного виявлення пожежі та пожежогасіння (далі – АПГ).

1.3. Система електроживлення має забезпечувати безперебійне електроживлення ПТК, в тому числі передбачати можливість автономної роботи (без отримання електроживлення із загальної мережі) протягом не менше ніж 48 годин.

2. Опис рівнів безпеки приміщень

2.1. Загальні вимоги до рівнів безпеки приміщень

У цих Вимогах визначається чотири рівні безпеки приміщень.

Вимоги до механізмів безпеки для кожного рівня безпеки наведено в порядку зростання таким чином, що рівень, наведений вище, передбачає виконання усіх вимог попереднього рівня.

Для кожного рівня безпеки механізми безпеки можуть бути посилені на підставі оцінених ризиків та виправдано обраних механізмів їх нейтралізації.

2.2. Рівень безпеки 1 приміщень

Рівень безпеки 1 приміщень передбачає реалізацію таких заходів:

1) організований перший периметр безпеки на вході та в зоні прийому відвідувачів в будівлі;

2) реалізований пропускний режим, який обмежує доступ відвідувачів до об'єктів розташованих на рівні безпеки 2;

3) впроваджена електронна система безпеки, яка забезпечує відеоспостереження замкнутого контуру:

входи та виходи у всіх точках доступу до будівлі надавача;

фіксування перебування/доступу до об'єктів надавача відвідувачами надавача.

2.2. Рівень безпеки 2 приміщень

Рівень безпеки 2 приміщень передбачає реалізацію таких заходів:

1) реалізований другий периметр безпеки, яким визначаються частини приміщення для роботи виключно персоналу надавача;

2) організоване перебування відвідувачів надавача в цій зоні безпеки вимагає наявності супроводу (охоронець або персонал надавача);

3) впроваджена електронна система безпеки, яка забезпечує відеоспостереження переходу до наступного рівня безпеки.

2.3. Рівень безпеки 3 приміщень

Рівень безпеки 3 приміщень передбачає реалізацію таких заходів:

1) приміщення цього рівня безпеки визначені, як зона обмеженого доступу, що передує (с буферною) для об’єктів надавача, які розміщені в зонах безпеки найвищого рівня;

2) персонал, який виконує функціональні обов’язки в робочій зоні (рівень безпеки 2), не має можливості перебувати біля входу до приміщення рівня безпеки 4;

3) доступ до цієї зони дозволений тільки персоналу, який відповідно до посадових обов’язків безпосередньо виконує завдання з підтримки та забезпечення функціонування критичних компонентів надавача для надання ним електронних довірчих послуг.

4) приміщення повинно відповідати таким вимогам:

стіни, підлога, стеля: в кладці, бетоні, цегляні або еквівалентні матеріали;

двері: антивандальні (стійкими до зловмисного зламу), броньовані металевими листами, з шарнірами, закріпленими в їх середині, з керованим ЕСБ замком, вогнестривкі, оснащені механізмами автоматично закриття (наприклад: доводчики, пружини);

вікна (якщо такі є) повинні бути захищені: від зовнішнього спостереження - матовою чи рельєфною поверхнею нерівностями назовні, непрозорими шторами тощо; від зовнішнього проникнення - сталевими прутами, які вставлені в стіну не менше ніж на 5 сантиметрів на відстані один від одного не більше 15 сантиметрів, детекторами розбиття скла;

5) в підсистемах ЕСБ повинні бути реалізовані такі заходи:

підсистема КД:

вхід/вихід з цієї зони безпеки здійснюється з використанням механізмів автентифікації, що базуються мінімум на двох факторах (наприклад: смарт карка та код кодового замка);

двері доступу до цієї зони повинні дозволяти вхід і вихід через активацію засувок, які працюють автоматично, після позитивної автентифікації, наданої підсистемою КД, а також надавати можливість їх ручного відмикання лише з середини та у випадку виникнення надзвичайних ситуацій;

підсистема ВВС:

зона безпеки повинна бути обладнана детекторами руху та датчиками відкриття/закриття дверей;

повинен видаватися сигнал тривоги при несанкціонованому переміщенні в межах зони, а також кожного разу, коли двері залишаються відчиненими більше 10 секунд;

підсистема ВСК:

зона повинна бути обладнана телекамерами, які забезпечують огляд дверей приміщення з нижчим рівнем безпеки та дверей приміщення з вищим рівнем безпеки, але з неможливістю візуалізації подій, що відбуваються в приміщенні з найвищим рівнем безпеки;

підсистема ПГ повинна бути обладнаною пожежними датчиками кількість яких відповідає розміру приміщення.

У разі неможливості обладнання цього рівня як окремого буферного приміщення на шляху до спеціального приміщення він обладнується у вигляді тамбура розміром не менше 4 м^2 з дотриманням усіх вимог встановлених для рівня безпеки 3.

2.4. Рівень безпеки 4 приміщень

Рівень безпеки 4 приміщень передбачає реалізацію таких заходів:

1) приміщення цього рівня безпеки визначені, як виокремлена територія надавача, де здійснюється його безпосередня діяльність, тобто – оперативна зона, є спеціальним приміщенням. Доступ до спеціального приміщення наданий та дозволений:

лише працівникам надавача, відповідно до їх функціональних обов'язків;

лише двом працівникам одночасно;

лише для працівників, які виконують різні функціональні обов'язки в структурі персоналу надавача (наприклад адміністратор безпеки та аудиту і системний адміністратор);

за умови обов'язкового запису в журналі відвідування цієї зони, який є невід'ємною частиною документації і зареєстрований надавачем, в якому зазначається: рік, місяць, день, час (з точністю до хвилини) входу/виходу персоналу та причина відвідування).

Персонал надавача, який не віднесений до персоналу виконання робіт в оперативній зоні, є відвідувачами спеціального приміщення.

Відвідувачі (в тому числі не з числа персоналу надавача) можуть отримати право доступу до оперативної зони виключно за документально оформленим рішенням керівника надавача, в якому вказуються ідентифікаційні дані таких осіб, причина надання їм доступу до оперативної зони та час, в який відвідувачі можуть отримати доступ до оперативної зони.

Доступ відвідувачів до спеціального приміщення може бути здійснено виключно в супроводі працівників з персоналу надавача, які мають право доступу до оперативної зони;

2) вимоги до приміщення рівня безпеки 4 надавача аналогічні вимогам до рівня безпеки 3, за винятком того, що у приміщеннях рівня безпеки 4 відсутні вікна;

3) якщо оперативна зона розташована у місці, що потенційно має загрозу затоплення, вона повинна бути обладнана датчиками протікання води;

4) в підсистемах ЕСБ повинні бути реалізовані такі заходи:

підсистема КД:

процедура входу/виходу в цій зоні вимагає використання механізмів ідентифікації, що базуються мінімум на двох факторах, один з яких обов'язково використовує технології на основі біометрії (на вході), які повинні бути налаштовані на зменшення рівня помилкової ідентифікації;

двері доступу до цієї зони повинні дозволяти вхід/вихід через активацію засувок, які працюють автоматично, після позитивної автентифікації, наданої підсистемою КД, здійснення процедури автентифікації для доступу до оперативної зони повинно бути доступним виключно після позитивної автентифікації доступу до попереднього рівня;

двері повинні надавати можливість їх ручного відмикання лише з середини та у випадку виникнення надзвичайних ситуацій;

підсистема ВВС повинна передбачати:

обладнання детекторами руху та датчиками відкриття/закриття дверей;

вмикання тривожного сигналу (ів) у випадку наявності в підсистемі КД інформації про порушення у межах оперативної зони, а також кожного разу, коли двері у/з цієї зони відкриті більше ніж 10 секунд;

підсистема ПГ повинна бути обладнаною пожежними датчиками кількість яких відповідає розміру приміщення та автоматичною системою пожежогасіння.

3. Вимоги до безпечного сховища

3.1. Безпечне сховище, що знаходиться в спеціальному приміщенні призначене для зберігання носіїв виключно критичної для надання послуг надавачем інформації (резервна копія особистого ключа надавача, засоби авторизації в ПТК надавача тощо).

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

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

3.4. Безпечне сховище повинне мати сертифікат про відповідність національному стандарту України 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».

4. Вимоги до ПТК

4.1. ПТК, що використовується під час надання електронних довірчих послуг, повинен забезпечувати:

1) функціонування системи моніторингу, що забезпечує збирання та аналіз інформації про стан критичних компонентів, в тому числі про вимкнення, запуск, перезапуск, доступність та рівень навантаження таких компонентів, виявлення та інформування про аномальну системну активність, що вказує на потенційне порушення системи безпеки;

2) реєстрацію подій встановлених підпунктом 6.1 пункту 6 розділу III цих Вимог, що можуть бути автоматизовані;

3) використання виключно ліцензійних комп'ютерних програм;

4) використання загальносистемних технічних та програмних засобів, що мають вбудовані функції контролю цілісності, автентифікації користувачів, ведення журналів подій, безпечного виконання операцій тощо;

5) використання засобів кваліфікованого електронного підпису чи печатки, які мають вбудовані апаратно-програмні засоби, що забезпечують захист записаних на них даних від несанкціонованого доступу, від безпосереднього ознайомлення із значенням параметрів особистих ключів та їх копіювання;

6) розподіл на сегменти (підсистеми) за функціональними, логічними та фізичними взаємозв'язками (включаючи місцезнаходження) між робочими

станціями та системами (службами) з встановленням елементів контролю безпеки відповідно до пункту 2 розділу IV цих Вимог.

4.2. Для всіх технічних та програмних засобів, розташованих у одному сегменті ПТК застосовуються однакові елементи контролю безпеки. Доступ і зв'язки між сегментами обмежуються тільки необхідними для правильного функціонування ПТК, а необов'язкові підключення повинні бути явно заборонені або деактивовані.

4.3. Локальний сегмент ПТК, який забезпечує управління надання послугами, та сегмент ПТК, який забезпечує взаємодію з користувачами, повинні бути розділені. Робочі станції, що використовуються для управління безпекою не повинні використовуватися для інших цілей.

V. Вимоги до оцінки ризиків

1. Оцінка ризиків

1.1. Процедури оцінки ризиків повинні включати 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 0,33 до 2 та обчислюється відповідно до пункту 4 розділу V цих Вимог,

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

«*» є математичною операцією множення.

1.3. Ризики, які приймають значення більше 3 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, а також інформація, яку надавач збирає та/або формує і зберігає із забезпеченням належного рівня довіри та відповідні процеси.

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

2.3. Після ідентифікації активів, здійснюється 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 віднесені до таких категорій:

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

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

2.5. До основних активів щонайменше повинні бути віднесені 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 ЕСБ.

2.6. До активів підтримки щонайменше повинні бути віднесені такі:

1) програмне забезпечення та обладнання ІТС надавача та ВПР:

апаратне забезпечення, на якому базується ПТК надавача;

програмне забезпечення, яке 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 веб-сайту 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, системи ЕСБ тощо);

клієнтська база надавача.

3. Визначення загроз

3.1. Процедури визначення загроз повинні включати заходи з виявлення загроз, оцінки ймовірності їх виникнення та наслідків. Визначення загроз здійснюється 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 не має наслідків для діяльності надавача.

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

3.3. За характером виникнення загрози можуть поділятись 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 відноситься 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 бути віднесені:

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, здійснення 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 бути віднесені:

електропостачання;

доступ до телекомунікаційних мереж;

обслуговування систем охолодження;

необхідне для роботи обладнання та/або розхідні матеріали.

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

До антропогенних загроз можуть бути віднесені:

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 бути віднесені:

зловмисники;

комп'ютерні злочинці;

шпигунські організації;

невдоволені працівники.

В 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. Визначення можливих вразливостей здійснюється 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 множення.

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

4.4. Надавачем здійснюються заходи нейтралізації загроз шляхом виконання вимог законодавства у сфері електронних довірчих послуг та вжиття інших адекватних заходів, відповідно до вимог стандартів у сфері інформаційної безпеки.

До заходів нейтралізації відносять ті заходи, які 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 бути віднесені:

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, яке 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 бути віднесені:

відсутність резервного копіювання особистих ключів надавача;

недостатній захист резервних копій особистих ключів надавача;

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

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

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 із значенням параметрів особистих ключів та їх копіювання.

4.8. До вразливостей механізмів перевірки факту володіння заявником особистим ключем та отримання від заявника відкритого ключа можуть бути віднесені:

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.

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

4.10. До вразливостей процесів забезпечення діяльності надавача можуть бути віднесені:

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

відсутність резервування телекомунікаційних мереж доступу;

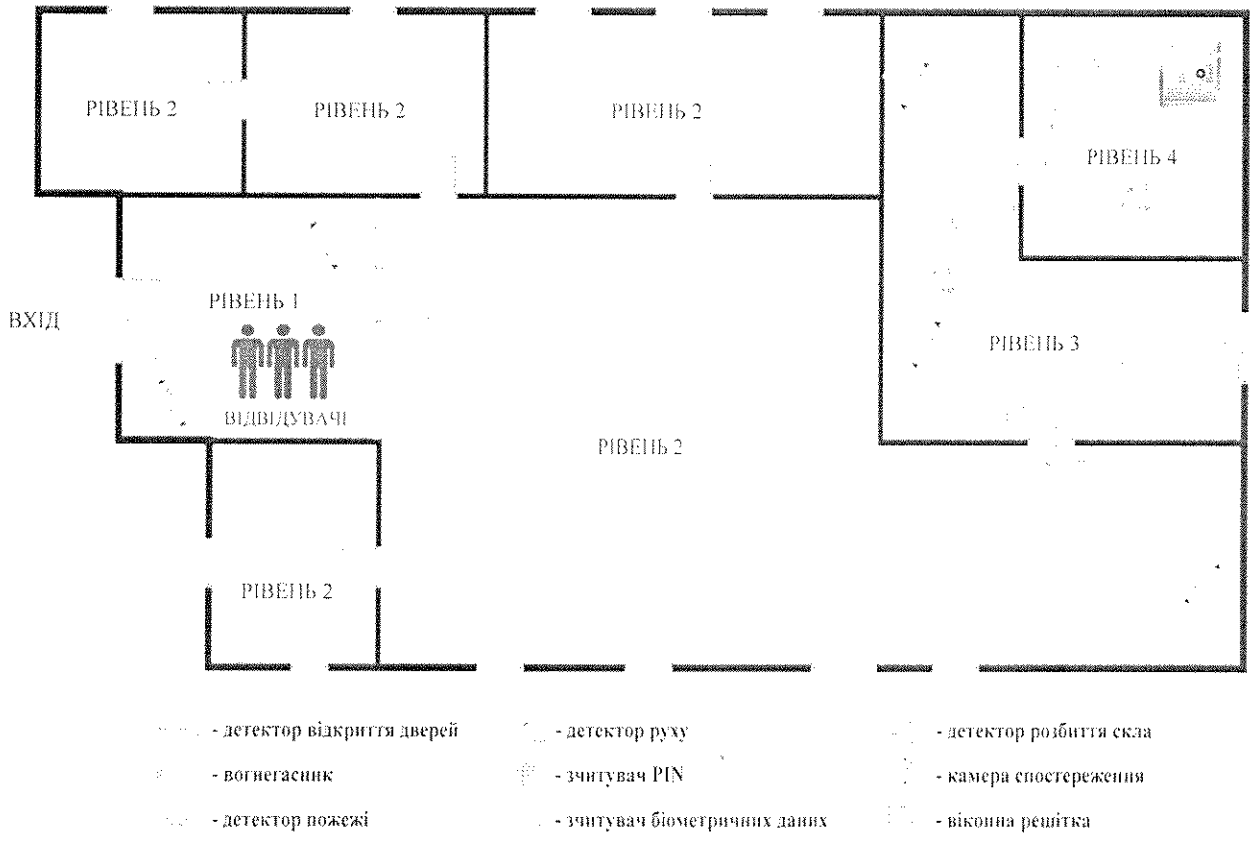
відсутність обліку та завчасного замовлення розхідних матеріалів, необхідних для роботи надавача;

експлуатація техніки та обладнання понад встановлені експлуатаційні терміни.

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

Додаток 1
до підпункту 1.1 пункту 1 розділу IV Вимог з безпеки та захисту інформації до кваліфікованих надавачів електронних довірчих послуг та їхніх відокремлених пунктів реєстрації

Приклад схематичного зображення рівнів безпеки та реалізуємих на цих рівнях механізмів безпеки



ПОЯСНОВАЛЬНА 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»;

абзацу другого підпункту 2 пункту 3 Положення про Адміністрацію Державної служби спеціального зв'язку та захисту інформації України, затвердженого постановою Кабінету Міністрів України від 03 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. Обґрунтування необхідності прийняття акта

Відповідно до абзацу третього частини другої статті 8 Закону України «Про електронні довірчі послуги» до повноважень спеціально уповноваженого центрального органу виконавчої влади з питань організації спеціального зв'язку та захисту інформації у сферах електронних довірчих послуг та електронної ідентифікації належить забезпечення встановлення вимог з безпеки та захисту інформації до кваліфікованих надавачів електронних довірчих послуг та їхніх відокремлених пунктів реєстрації.

Пунктом 37 частини першої статті 14 Закону України «Про Державну службу спеціального зв'язку та захисту інформації України» визначено, що на Державну службу спеціального зв'язку та захисту інформації України відповідно до визначених завдань покладаються обов'язки щодо встановлення вимог з безпеки та захисту інформації до кваліфікованих надавачів електронних довірчих послуг та їхніх відокремлених пунктів реєстрації.

Прийняття наказу забезпечить врегулювання питань встановлення належного рівня безпеки та захисту інформації при наданні кваліфікованих електронних довірчих послуг.

3. Суть проекту акта

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). Враховуючи вимоги Закону України «Про електронні довірчі послуги» та Вимоги у сфері електронних довірчих послуг, затверджені постановою Кабінету Міністрів України від 07 листопада 2018 року № 992, проектом наказу деталізовано та визначено спосіб забезпечення безпеки та захисту інформації кваліфікованих надавачів електронних довірчих послуг (далі – надавач) та відокремлених пунктів реєстрації (далі – ВПР).

Проектом наказу передбачено, що забезпечення безпеки інформації надавача або ВПР досягається 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.

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 03 вересня 2014 року № 411.

У цій сфері правового регулювання діють Закони України «Про електронні довірчі послуги», «Про основні засади забезпечення кібербезпеки України», «Про захист інформації в інформаційно-телекомунікаційних системах».

4-1. Відповідність засадам реалізації органами виконавчої влади принципів державної політики цифрового розвитку.

У проекті наказу відсутні положення, які не узгоджуються із засадами реалізації органами виконавчої влади принципів державної політики цифрового розвитку.

Проект наказу не стосується питань інформатизації, електронного урядування, формування і використання національних електронних інформаційних ресурсів, розвитку інформаційного суспільства, електронної демократії, надання адміністративних послуг або цифрового розвитку.

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 надавачів та посиленням заходів захисту інформаційно-телекомунікаційних систем надавачів та ВІР.

На сьогодні в Україні функціонують 6 надавачів, які фінансуються за рахунок державного бюджету.

Вартість реалізації одним надавачем (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 Держспецзв'язку у розділі «Регуляторна діяльність» у підрозділі «Повідомлення про оприлюднення та проекти»).

6. Прогноз впливу

Проект наказу є регуляторним актом.

Реалізація наказу 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.

Прогноз впливу реалізації акта на ключові інтереси заінтересованих сторін додається.

Реалізація проекту 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;

інші сфери суспільних відносин.

6-1. Стратегічна екологічна оцінка

Проектом наказу не затверджується документ державного планування, підготовлений з урахуванням особливостей, передбачених Законом України «Про стратегічну екологічну оцінку».

7. Позиція заінтересованих сторін

Проект наказу потребує консультацій з суб'єктами господарювання, що надають або мають намір надавати кваліфіковані електронні довірчі послуги, оскільки матиме на них вплив. У зв'язку з цим проект наказу розміщено на офіційному веб-сайті Держспецзв'язку.

Проект наказу матиме вплив на інтереси заінтересованих сторін, про що зазначено в прогнозі впливу, що додається.

За предметом правового регулювання проект наказу не стосується:

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

соціально-трудової сфери;

сфери наукової та науково-технічної діяльності.

8. Громадське обговорення

Проект наказу потребує проведення консультацій з громадськістю та розміщено на офіційному веб-сайті Держспецзв'язку.

9. Позиція заінтересованих органів

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

10. Правова експертиза

Проект наказу потребує проведення державної реєстрації в Міністерстві юстиції України.

11. Запобігання дискримінації

У проекті наказу відсутні положення, які містять ознаки дискримінації.

Проект наказу не потребує проведення громадської антидискримінаційної експертизи.

11-1. Відповідність принципу забезпечення рівних прав та можливостей жінок і чоловіків

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

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

Реалізація наказу сприятиме:

підвищенню рівня довіри фізичних та юридичних осіб до кваліфікованих електронних довірчих послуг;

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

забезпеченню належного рівня захисту інформації та персональних даних, що обробляються під час надання електронних довірчих послуг.

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

«04» 07 2019 року

ПРОГНОЗ ВПЛИВУ
реалізації акта на ключові інтереси заінтересованих сторін

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»

1. Короткий опис суті проекту

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, щодо забезпечення безпеки та захисту інформації кваліфікованих надавачів електронних довірчих послуг (далі – надавач) та відокремлених пунктів реєстрації (далі – ВПР) під час надання ними кваліфікованих електронних довірчих послуг (далі – послуги).

Проектом наказу передбачено забезпечення безпеки інформації надавача або ВПР шляхом комплексного застосування необхідного набору взаємодоповнюючих заходів щодо захисту інформації в інформаційно-телекомунікаційних системах 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.

2. Вплив на ключові інтереси усіх заінтересованих сторін

Заінтересована сторона	Ключовий інтерес	Очікуваний вплив на ключовий інтерес із зазначенням передбачуваної динаміки змін основних показників		Пояснення
		Короткостроковий вплив (до року)	Середньостроковий вплив (більше року)	
Громадяни	Підвищення рівня довіри до послуг	позитивний	позитивний	Відповідність послуг міжнародним стандартам для високого рівня довіри
Держава	Підвищення рівня довіри до послуг та кіберзахисту обєктів, що їх використовують	позитивний	позитивний	Відповідність послуг міжнародним стандартам для високого рівня довіри
Суб'єкти господарювання	Створення умов та забезпечення надання послуг відповідно до єдиних підходів з виконання вимог міжнародних стандартів з безпеки та захисту інформації	негативний (витрати на модернізацію ІТС та впровадження організаційних заходів)	позитивний (підвищення конкурентноспроможності, захищеність від кіберзагроз)	Відповідність послуг міжнародним стандартам для високого рівня довіри

Голова Державної служби спеціального зв'язку та захисту інформації України
«04» 07 2019 року

Леонід Євдоченко

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; підвищення рівня довіри	Прийняття проекту наказу: потребуватиме збільшення видатків з державного бюджету внаслідок запровадження додаткових організаційно-методологічних, технічних та технологічних умов діяльності кваліфікованих надавачів електронних

	до кваліфікованих електронних довірчих послуг.	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 проекту наказу	Прийняття проекту наказу матиме такий вплив на інтереси громадян:	Прийняття проекту наказу може призвести до збільшення вартості

	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.	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 обслуговування, навчання / підвищення кваліфікації персоналу тощо, гривень:**	**145 700,00**	**160 700,00**
1.1.	проведення модернізації комплексної	130 700,00	130 700,00

	системи захисту інформації в інформаційно-телекомунікаційній системі кваліфікованого надавача електронних довірчих послуг (придбання обладнання, приладів та ліцензійного програмного 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,**	**1 000,00**	**5 000,00**

	канцелярські товари тощо), гривень		
6.	**Витрати, пов'язані із наймом додаткового персоналу, гривень:**	**44 700,00**	**223 500,00**
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 2018 року – 3723,00 гривні)	44 700,00	223 500,00
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 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 кваліфікованих електронних довірчих послуг; збільшенню прибутку суб'єкта	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	Цілі, визначені стратегічним документами досягнуті

	господарювання.	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	Планові витрати часу на процедуру	Вартість часу співробітника органу державної влади	Оцінка кількості процедур за рік, що припадають	Оцінка кількості суб'єктів, що підпадають під дію	Витрати на адміністрування регулювання (за рік), гривень

підприємництва (розрахунок на одного типового суб'єкта господарювання)		відповідної категорії (заробітна плата)	на одного суб'єкта	процедури регулювання	
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 оприлюднення одного окремого акта про порушення	**1 робочий день**	**400,00 грн за робочий день (з розрахунку 9 000,00 грн за місяць)**	**1**	**24**	**400,00**

вимог регулювання (Адміністрація Державної служби спеціального зв'язку та захисту інформації України)					
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 інформації України	1 робочий день	400,00 грн за робочий день (з розрахунку 9 000,00 грн за місяць)	1	24	400,00
Міністерство юстиції України	1 робочий день	400,00 грн за робочий день (з розрахунку 9 000,00 грн за місяць)	1	24	400,00
6. Підготовка звітності за результатами регулювання (Адміністрація Державної	**2 робочі дні**	**400,00 грн за робочий день (з розрахунку 9 000,00 грн за місяць)**	**1**	**24**	**800,00**

служби спеціального зв'язку та захисту інформації України)					
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. 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 **Леонід Євдоченко**

«04» 07 2019 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

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.

3. Обраний спосіб оприлюднення проекту акта

Проект акта та аналіз регуляторного впливу розміщено на веб-сайті Держспецзв'язку.

4. Строк, протягом якого приймаються зауваження та пропозиції

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

Голова Державної служби спеціального
зв'язку та захисту інформації України Леонід Євдоченко
«04» 07 2019 р.