Прим. № __

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

24.09.2019 № 04/02/03-2744

Державна регуляторна служба України

вул. Арсенальна, 9/11, м. Київ, 01011

Щодо погодження проєкту
наказу Адміністрації Держспецзв'язку

З метою приведення нормативно-правових актів Державної служби спеціального зв'язку та захисту інформації України у відповідність із Законом України «Про електронні довірчі послуги» розроблено проєкт наказу Адміністрації Держспецзв'язку «Про затвердження Змін до деяких наказів Адміністрації Державної служби спеціального зв'язку та захисту інформації України».

Просимо розглянути та погодити проєкт наказу до 26 вересня 2019 року.

Додатки:
1. Проект наказу від 19.09.2019 № 04/02/03-2708 прим. № 4 на 18 арк.
2. Порівняльна таблиця від 19.09.2019 № 04/02/03-2709 прим. № 4 на 27 арк.
3. Пояснювальна записка від 19.09.2019 № 04/02/03-2710 прим. № 4 на 7 арк.
4. Аналіз регуляторного впливу проекту наказу від 23.09.2019 № 04/02/03-2743 прим. № 1 на 11 арк.
5. Повідомлення про оприлюднення на 1 арк.
6. Протокол узгодження позицій на 26 арк.

Перший заступник Голови Служби Олександр ЧАУЗОВ

Вик. Ткаченко Я.Е.
тел. 281-97-47

0.31

ПРОЄКТ
Прим. № 4

АДМІНІСТРАЦІЯ ДЕРЖАВНОЇ СЛУЖБИ СПЕЦІАЛЬНОГО ЗВ'ЯЗКУ ТА ЗАХИСТУ ІНФОРМАЦІЇ УКРАЇНИ

Н А К А З

м. Київ

___.___.20__ № ____

Про затвердження Змін до деяких наказів Адміністрації Державної служби спеціального зв'язку та захисту інформації України

Відповідно до 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, та з метою удосконалення нормативно-правових актів у сфері криптографічного захисту інформації та приведення їх у відповідність до законодавства

НАКАЗУЮ:

1. Затвердити Зміни до деяких наказів Адміністрації Державної служби спеціального зв'язку та захисту інформації України, що додаються.

2. Визнати такими, що втратили чинність:

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

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

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

4. Цей наказ набирає чинності з дня його офіційного опублікування, крім пунктів 1 та 2 Змін до деяких наказів Адміністрації Державної служби спеціального зв'язку та захисту інформації України, що затверджується цим наказом, які набирають чинності через шість місяців з дня офіційного опублікування цього наказу.

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

Голова Служби Леонід ЄВДОЧЕНКО

Леонід ЄВДОЧЕНКО

ПРОЄКТ

ЗАТВЕРДЖЕНО

Наказ Адміністрації Державної служби спеціального зв'язку та захисту інформації України
__ _____ 2019 року № _____

Зареєстровано в Міністерстві юстиції України
__.__.2019 за № _____/_____

Зміни
до деяких наказів Адміністрації Державної служби спеціального зв'язку та захисту інформації України

1. У Положенні про порядок розроблення, виробництва та експлуатації засобів криптографічного захисту інформації, затвердженому наказом Адміністрації Державної служби спеціального зв'язку та захисту інформації України від 20 липня 2007 року № 141, зареєстрованому в Міністерстві юстиції України 30 липня 2007 року за № 862/14129 (у редакції наказу Адміністрації Державної служби спеціального зв'язку та захисту інформації України від 14 грудня 2015 року № 767):

1) у розділі I:

пункт 1 викласти у такій редакції:

«1. Це Положення визначає вимоги до порядку розроблення, виробництва та експлуатації засобів криптографічного захисту державних інформаційних ресурсів або інформації, вимога щодо захисту якої встановлена законом,

засобів удосконаленого електронного підпису чи печатки, засобів кваліфікованого електронного підпису чи печатки, засобів, спеціально призначених для розроблення, дослідження, виробництва та випробування засобів криптографічного захисту інформації (далі – засоби КЗІ).

Особливості розроблення, виготовлення, уведення в експлуатацію та експлуатації засобів КЗІ, призначених для криптографічного захисту інформації, що становить державну таємницю, та службової інформації визначаються відповідно до чинного законодавства.

Розроблення засобів КЗІ, що фінансується за рахунок коштів Державного бюджету України, погоджується з Адміністрацією Державної служби спеціального зв'язку та захисту інформації України (далі - Адміністрація Держспецзв'язку).

Національний банк України може розробляти засоби КЗІ, призначені виключно для забезпечення власних потреб та потреб банківської системи України, без погодження з Адміністрацією Держспецзв'язку.»;

у пункті 2 слова «надійних засобів електронного цифрового підпису та засобів, спеціально призначених для розроблення, дослідження, виробництва та випробування засобів КЗІ» виключити;

у пункті 4:

абзац сьомий після слів «криптографічне перетворення інформації» доповнити словами «(далі – криптоперетворення)», та після слів «інформації з використанням» доповнити словами «криптографічних алгоритмів та»;

у абзаці дванадцятому слова «нормативних документів у сфері КЗІ» замінити словами «законодавства та нормативних документів у сферах захисту інформації та інформаційної безпеки»;

у абзаці шістандцятому слова «сфері криптографічного захисту інформації та у сфері електронного цифрового підпису» замінити словами «сферах захисту інформації та електронних довірчих послуг»;

абзац шістнадцятий пункту 5 викласти у такій редакції:

«засоби, що реалізують криптоперетворення та/або механізми імітозахисту, та призначені для забезпечення захисту (підтвердження) хоча б однієї з таких властивостей інформації: справжності (авторства), цілісності, неспростовності, дати створення (далі - засоби категорії «П»);»

у пункті 8 слова «послуг електронного цифрового підпису» замінити словами «електронних довірчих послуг»;

у пункті 9 слова «сфері КЗІ» замінити словами «сферах захисту інформації та інформаційної безпеки».

2) у розділі ІІ:

пункт 1 викласти у такій редакції:

«1. Розроблення засобів КЗІ здійснюється відповідно до вимог нормативно-правових актів у сферах захисту інформації та інформаційної безпеки, розроблення та поставлення продукції на виробництво»;

у пункті 10:

у абзаці першому слово «типу» виключити;

абзац двадцятий виключити;

абзац двадцять третій пункту 10 викласти у такій редакції:

«Вимоги до засобів кваліфікованого електронного підпису чи печатки, визначаються Вимогами у сфері електронних довірчих послуг, затвердженими постановою Кабінету Міністрів України від 7 листопада 2018 р. № 992, наказами Міністерства юстиції України та Адміністрації Держспецзв'язку»;

у абзаці третьому пункту 12 слова «сфері КЗІ» замінити словами «сфері криптографічного захисту інформації (далі – КЗІ)»;

у пункті 15:

у абзаці першому слова «практична реалізація» замінити словами «реалізація функцій захисту відповідних проєктних рішень»;

у абзаці п'ятому слово «електронного» виключити;

3) у розділі IV:

пункт 1 викласти у такій редакції:

«1. Для криптографічного захисту державних інформаційних ресурсів або інформації, вимога щодо захисту якої встановлена законом, використовуються засоби КЗІ, які мають документ про відповідність або позитивний експертний висновок за результатами державної експертизи у сфері КЗІ, що підтверджують клас засобу КЗІ (рівень гарантій) та реалізовані методи захисту, а суб'єкти, що їх використовують, мають на це права.

Оцінка відповідності та державна експертиза у сфері криптографічного захисту інформації проводяться в порядку, визначеному відповідними нормативно-правовими актами.»;

пункт 3 доповнити новим абзацом такого змісту:

«Особливості обліку засобів удосконаленого електронного підпису чи печатки, засобів кваліфікованого електронного підпису чи печатки та носіїв ключової інформації до них визначаються нормативно-правовими актами у сфері електронних довірчих послуг».

2. У Положенні про державну експертизу в сфері криптографічного захисту інформації, затвердженому наказом Адміністрації Державної служби спеціального зв'язку та захисту інформації України від 23 червня 2008 року

№ 100, зареєстрованому в Міністерстві юстиції України 16 липня 2008 року за № 651/15342 (зі змінами):

1) у розділі І:

абзац одинадцятий пункту 1.3 викласти в такій редакції:

«Інші терміни вживаються у значенні, наведеному в Законах України «Про Державну службу спеціального зв'язку та захисту інформації України», «Про захист інформації в інформаційно-телекомунікаційних системах», «Про електронні довірчі послуги», Положенні про порядок здійснення криптографічного захисту інформації в Україні, затвердженому Указом Президента України від 22 травня 1998 року № 505, Положенні про порядок розроблення, виробництва та експлуатації засобів криптографічного захисту інформації, затвердженому наказом Адміністрації Державної служби спеціального зв'язку та захисту інформації України від 20 липня 2007 року № 141, зареєстрованому у Міністерстві юстиції України 30 липня 2007 року за № 862/14129 (із змінами).»;

у абзаці шостому пункту 1.5 слова «, програмно-технічні комплекси центрів сертифікації ключів, надійні засоби електронного цифрового підпису» виключити;

у пункті 1.6:

абзац п'ятий пункту викласти в такій редакції:

«криптосистеми, засоби й обладнання криптографічного захисту державних інформаційних ресурсів або інформації, вимога щодо захисту якої встановлена законом, криптосистеми, що використовуються для надання кваліфікованих електронних довірчих послуг, або в схемах електронної ідентифікації, засоби удосконаленого електронного підпису чи печатки, засоби кваліфікованого електронного підпису чи печатки;»;

доповнити абзацами шість та сім такого змісту:

«засоби, що реалізують криптоперетворення та/або механізми імітозахисту, та використовуються в системах зв'язку, управління та озброєння;

засоби обробки та передачі державних інформаційних ресурсів або інформації, вимога щодо захисту якої встановлена законом, які реалізують функції криптографічного захисту інформації;»;

2) у абзаці четвертому підпункту 2.1.1 пункту 2.1 розділу II слова «програмно-технічні комплекси центрів сертифікації ключів, які передбачають акредитацію, надійні засоби електронного цифрового підпису» замінити словами «засоби удосконаленого електронного підпису чи печатки, засоби кваліфікованого електронного підпису чи печатки»;

3) у додатку 2:

у абзаці другому пункту 8 слова «та технічні умови (згідно ДСТУ 1.3:2004 «Національна стандартизація. Правила побудови, викладання, оформлення, погодження, прийняття та позначення технічних умов, ДСТУ – Н 4486:2005 Система конструкторської документації. Настанова щодо типової побудови технічних умов, ГОСТ 2.114-95 «Единая система конструкторской документации. Технические условия»)» виключити;

у пункті 9:

у абзаці другому слова «(згідно з ГОСТ 19.201-78 «Единая система документации. Техническое задание. Требования к содержанию и оформлению»)» виключити;

у абзаці третьому слова «(згідно з ДСТУ 1.3:2004 Національна стандартизація. Правила побудови, викладання, оформлення, погодження, прийняття та позначення технічних умов (за потреби)» виключити;

в абзаці четвертому слова «(згідно з ГОСТ 19.202-78 «Единая система программной документации. Спецификация. Требования к содержанию и оформлению»)» виключити;

в абзаці п'ятому слова «(згідно з ГОСТ 19.401-78 «Единая система программной документации. Текст программы. Требования к содержанию и оформлению»)» виключити;

в абзаці шостому слова «(згідно з ГОСТ 19.402-78 «Единая система программной документации. Описание программы»)» виключити;

в абзаці сьомому слова «(згідно з ГОСТ 19.301-79 «Единая система программной документации. Программа и методика испытаний. Требования к содержанию и оформлению»)» виключити;

в абзаці восьмому слова «(згідно з ГОСТ 19.503-79 «Единая система программной документации. Руководство системного программиста. Требования к содержанию и оформлению»)» виключити;

в абзаці дев'ятому слова «(згідно з ГОСТ 19.504-79 «Единая система программной документации. Руководство программиста. Требования к содержанию и оформлению»)» виключити;

в абзаці десятому слова «(згідно з ГОСТ 19.505-79 «Единая система программной документации. Руководство оператора. Требования к содержанию и оформлению»)» виключити;

3. У наказі Адміністрації Державної служби спеціального зв'язку та захисту інформації України від 18 грудня 2012 року № 739, зареєстрованому в Міністерстві юстиції України 14 січня 2013 року за № 108/22640 (зі змінами):

пункт 2 викласти у такій редакції:

«2. Установити, що державні органи при електронній взаємодії, що здійснюється з використанням кваліфікованих електронних довірчих послуг, при здійсненні обміну електронних даних конфіденційного характеру через глобальні мережі передачі даних, забезпечують конфіденційність таких даних з використанням засобів криптографічного захисту інформації та сертифікатів шифрування, що відповідають Вимогам»;

пункт 3 викласти у такій редакції:

«3. Установити, що кваліфіковані надавачі електронних довірчих послуг мають право надавати послуги з обслуговування сертифікатів шифрування, та у разі фактичного їх надання інформують про це Адміністрацію Держспецзв'язку.»;

пункт 4 виключити;

пункти 5, 6, 7 вважати відповідно пунктами 4, 5, 6.

4. У Вимогах до форматів криптографічних повідомлень, затверджених наказом Адміністрації Державної служби спеціального зв'язку та захисту інформації України від 18 грудня 2012 року № 739, зареєстрованих в Міністерстві юстиції України 14 січня 2013 року за № 108/22640 (зі змінами):

1) у розділі I:

у пункті 1.1 слова «та надійних засобів електронного цифрового підпису (далі – ЕЦП)» виключити;

пункт 1.2 викласти у такій редакції:

«1.2. Положення цих Вимог є обов'язковими для засобів КЗІ, призначених для забезпечення конфіденційності інформації з використанням сертифіката шифрування. Правильність реалізації у засобах КЗІ цих Вимог повинна бути підтверджена документом про відповідність або позитивним експертним висновком за результатами державної експертизи у сфері КЗІ.

Оцінка відповідності та державна експертиза у сфері КЗІ проводяться в порядку, визначеному відповідними нормативно-правовими актами.»;

у пункті 1.3:

у абзаці п'ятому слова «у циклічній групі поля або» виключити;

доповнити після абзацу п'ятого новим абзацом такого змісту:

«сертифікат шифрування – сертифікат відкритого ключа виданий надавачем електронних довірчих послуг та призначений для використання у протоколі узгодження ключа;»;

абзац дев'ятий викласти у такій редакції:

«Інші терміни вживаються у значеннях, наведених у Законі України «Про електронні довірчі послуги» та нормативно-правових актах у сфері електронних довірчих послуг;

у пункті 1.4:

абзац третій виключити;

абзац четвертий після слова «протокол» доповнити словами «узгодження ключів»;

у пункті 1.5:

у абзаці першому слова «ГОСТ 34.310-95 «Информационная технология. Криптографическая защита информации. Процессы выработки и проверки электронной цифровой подписи на базе ассиметричного криптографического алгоритма» (далі – ГОСТ 34.310-95),» виключити;

у абзаці другому абревіатуру «ЕЦП» замінити словами «цифрового підпису»;

пункт 1.8 викласти у такій редакції:

«1.8. Ці Вимоги розроблено з урахуванням Інструкції про порядок постачання і використання ключів до засобів криптографічного захисту інформації, затвердженої наказом Адміністрації Державної служби спеціального зв'язку та захисту інформації України від 12 червня 2007 року № 114, зареєстрованої в Міністерстві юстиції України 25 червня 2007 року за № 729/13996 (далі – Інструкція № 114), Вимог до електронних довірчих послуг,

затверджених постановою Кабінету Міністрів України від 07 листопада 2018 року № 992 (далі – Вимоги до електронних довірчих послуг).»;

пункт 1.9 виключити.

2) у розділі II:

пункт 2.2 викласти у такій редакції:

«2.2 Тип повідомлення «ContentInfo» подано в нотації ASN.1, яка визначена ДСТУ ISO/IEC 8824-1:2017 (ISO/IEC 8824-1:2015, IDT) «Інформаційні технології. Нотація абстрактного синтаксису 1 (ASN.1). Частина 1. Специфікація базової нотації», ДСТУ ISO/IEC 8824-2:2017 (ISO/IEC 8824-2:2015, IDT) «Інформаційні технології. Нотація абстрактного синтаксису 1 (ASN.1). Частина 2. Специфікація інформаційного об'єкта», ДСТУ ISO/IEC 8824-3:2008 (ISO/IEC 8824-3:2002, IDT) «Інформаційні технології. Нотація абстрактного синтаксису 1 (ASN.1). Частина 3. Специфікація обмежень», ДСТУ ISO/IEC 8824-4:2017 (ISO/IEC 8824-4:2015, IDT) «Інформаційні технології. Нотація абстрактного синтаксису 1 (ASN.1). Частина 4. Параметризація специфікацій ASN.1»;

у абзаці першому пункту 2.7 слова «формату підписаних даних» замінити словами «електронних довірчих послуг»;

3) пункт 3.2 глави 3 розділу III викласти у такій редакції:

«3.2. Для формування повідомлення «захищені дані» застосовується статичний або динамічний механізм узгодження ключів за протоколом Діффі-Геллмана.

3.2.1 Статичний механізм узгодження ключів («Static-Static mode») – узгодження ключів за протоколом Діффі-Геллмана, за якого як відправник, так і одержувач мають статичну ключову пару, відкритий ключ якої засвідчено кваліфікованим надавачем електронних довірчих послуг.

Статичний механізм узгодження ключів може використовуватися лише у випадку, коли параметри криптографічного алгоритму статичної ключової пари відправника еквівалентні параметрам криптографічного алгоритму статичної ключової пари одержувача. Якщо зазначені параметри не еквівалентні, повинен застосовуватися динамічний механізм узгодження ключів.

При статичному механізмі узгодження ключа для формування узгодженого ключа відправник повинен використовувати особистий ключ відправника та відкритий ключ одержувача. Одержувач повинен використовувати особистий ключ одержувача та відкритий ключ відправника.

Відкриті ключі відправника та одержувача обираються із сертифікатів шифрування.

3.2.2. Під час динамічного механізму узгодження ключа для формування узгодженого ключа відправник повинен використовувати особистий сеансовий ключ відправника і відкритий ключ одержувача. Одержувач повинен використовувати особистий ключ одержувача і відкритий сеансовий ключ відправника, що отримує від відправника, під час кожного сеансу в полі «originatorKey» структури «RecipientInfo».

При цьому параметри криптографічного алгоритму динамічної ключової пари відправника повинні бути еквівалентні параметрам криптографічного алгоритму статичної ключової пари одержувача.

При динамічному механізмі узгодження ключа для формування узгодженого ключа відправник повинен використовувати особистий ключ відправника і відкритий ключ одержувача. Одержувач повинен використовувати особистий ключ одержувача і відкритий ключ відправника, що отримується від відправника, при кожному сеансі у полі «originatorKey» структури «RecipientInfo».

Особливості кодування параметрів протоколу узгодження ключа визначено у главі 4 розділу V цих Вимог.

Протокол узгодження ключів Діффі-Геллмана в групі точок еліптичної кривої використовується для ключових пар (відправника та одержувача), що відповідають ДСТУ 4145-2002.»;

4) у главі 3 розділу IV:

пункт 3.2 викласти у такій редакції:

«3.2. Поле «originatorInfo» містить сертифікат шифрування відправника та додатково може містити пов'язані з ним кваліфіковані сертифікати відкритих ключів і списки відкликаних сертифікатів. Поле є необов'язковим.»;

підпункт 3.3.1 пункту 3.3 викласти у такій редакції:

«3.3.1. Поле «certs» містить сертифікат шифрування відправника та додатково може містити пов'язані з ним кваліфіковані сертифікати відкритих ключів для побудови шляху сертифікації від довіреного «кореня». Сертифікати розміщуються в такому порядку: першим (з найменшим індексом) розміщується кваліфікований сертифікат відкритого ключа вищого рівня (кореневий), останнім (з найбільшим індексом) розміщується сертифікат шифрування відправника, який було застосовано для статичного механізму.»;

підпункт 3.4.1 пункту 3.4 викласти у такій редакції:

«3.4.1. Поле «crls» містить набір списків відкликаних сертифікатів (CRL). Набір CRL містить інформацію, достатню для того, щоб визначити, чи є сертифікати в полі «certs» чинними. Послідовність розміщення CRL у полі «crls» повинна відповідати послідовності розміщення сертифікатів у наборі «certs». Наявність списків відкликаних сертифікатів дає змогу одержувачу визначити чинність сертифіката шифрування відправника на момент формування захищених даних без необхідності звернення до зовнішніх джерел розміщення CRL.»;

у пункті 3.7:

у підпункті 3.7.4:

у підпункті 3:

у абзаці другому слова «центру сертифікації» замінити словами «надавача електронних довірчих послуг»;

абзаци чотири – дев'ять виключити;

абзац третій підпункту 4 виключити;

у підпункті 3.7.5:

підпункт 3 виключити;

у абзаці тридцять п'ятому підпункту 4 цифру «4» замінити цифрою «3»;

підпункт 4 вважати підпунктом 3;

5) у розділі V:

абзац третій глави 1 викласти у такій редакції:

«У цих Вимогах визначено протокол узгодження ключа Діффі-Геллмана у групі точок еліптичної кривої (ECDH).»;

у абзаці п'ятому глави 2 та абзаці дванадцятому глави 3 слова «для визначеного протоколу в циклічній групі поля або в групі точок еліптичної кривої» виключити;

у главі 4:

пункт 4.1 виключити;

пункти 4.2, 4.3 вважати відповідно пунктами 4.1, 4.2;

пункт 4.2 викласти у такій редакції:

«4.2. Кодування ДКЕ виконується як:

dke OCTET STRING.

Для ДСТУ 4145-2002 ДКЕ кодується в упакованому форматі.

За відсутності ДКЕ в параметрах криптоалгоритму використовується ДКЕ № 1 Переліку ДКЕ, які рекомендуються до застосування у засобах КЗІ, наведеному у додатку 1 до Інструкції № 114.

Спосіб представлення ДКЕ № 1 повинен відповідати вимогам до технічних засобів, процесів їх створення, використання та функціонування у складі інформаційно-телекомунікаційних систем під час надання кваліфікованих електронних довірчих послуг, встановлених у нормативно-правових актах Мін'юсту та Адміністрації Держспецзв'язку.»;

у главі 5:

пункт 5.1 виключити;

пункти 5.2, 5.3 вважати відповідно пунктами 5.1, 5.2;

у пункті 5.2 цифри «5.2» замінити цифрами «5.1»;

у абзаці сьомому пункту 5.2 слова «у циклічній групі простого поля та у групі точок еліптичної кривої» виключити;

у главі 6:

пункт 6.3 виключити;

пункт 6.4 вважати пунктом 6.3;

у пункті 6.3:

підпункт 1 викласти у такій редакції:

«1) KDF-функція в групі точок еліптичної кривої (ECDH) ґрунтується на ДСТУ ISO/IEC 11770-3:2015.»;

у абзаці четвертому підпункту 2 цифру «4» замінити цифрою «3».

у підпункті 4:

у абзаці третьому виключити слова та цифри «(аналогічний полю «partyAInfo» структури «OtherInfo», наведеної у позиції 3 пункту 6.3 глави 6 розділу V цих Вимог)»;

у абзаці четвертому виключити слова та цифри «(аналогічно полю «suppPubInfo» структури «OtherInfo», наведеної у позиції 3 пункту 4.1 глави 4 розділу V)»;

6) у главі 4 розділу VI слова та абревіатури «алгоритмами узгодження ключа DH або» замінити словом «алгоритмом»;

7) у розділі VIII:

пункт 8.1 викласти у такій редакції:

«8.1 Сертифікат шифрування у цих Вимогах призначається для використання у протоколі узгодження ключа Діффі-Геллмана в групі точок еліптичної кривої.»;

пункт 8.2 викласти у такій редакції:

«8.2 Формат сертифіката шифрування повинен відповідати формату кваліфікованого сертифіката відкритого ключа, встановленого у Вимогах до електронних довірчих послуг»;

у абзацах восьмому – десятому пункту 8.3 слово «електронний» виключити.

5. У Інструкції про порядок постачання і використання ключів до засобів криптографічного захисту інформації, затвердженій наказом Адміністрації Державної служби спеціального зв'язку та захисту інформації України від 12 червня 2007 року № 114, зареєстрованій в Міністерстві юстиції України 25 червня 2007 року за № 729/13996 (зі змінами):

1) за текстом слова та цифри «ГОСТ 28147-89» замінити словами та цифрами «ДСТУ ГОСТ 28147:2009»;

2) у главі 1:

у пункті 1.1 слова «електронний цифровий підпис» замінити словами «електронні довірчі послуги»;

у пункті 1.3 слова «послуги електронного цифрового підпису» замінити словами «електронні довірчі послуги»;

у пункті 1.5:

у абзаці третьому слова «засобів електронного цифрового підпису» замінити словами «засобів удосконаленого електронного підпису чи печатки, засобів кваліфікованого електронного підпису чи печатки»;

у абзаці дев'ятому слова «електронного цифрового підпису» замінити словами «електронних довірчих послуг»;

3) у пункті 2.4 глави 2 слова «посилених» та «електронного цифрового підпису» виключити.

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

04/08/03-2708
19.09.19

Прим. № 4

ПОРІВНЯЛЬНА ТАБЛИЦЯ
до проєкту наказу Адміністрації Держспецзв'язку «Про затвердження Змін до деяких наказів Адміністрації Державної служби спеціального зв'язку та захисту інформації України»

Зміст положення (норми) чинного акта законодавства	Зміст відповідного положення (норми) проєкту акта
Наказ Адміністрації Держспецзв'язку від 20 липня 2007 року № 141 «Про затвердження Положення про порядок розроблення, виробництва та експлуатації засобів криптографічного захисту інформації», зареєстрований в Міністерстві юстиції України 30 липня 2007 року за № 862/14129 (у редакції наказу Адміністрації Державної служби спеціального зв'язку та захисту інформації України від 14 грудня 2015 року № 767)	
Положення про порядок розроблення, виробництва та експлуатації засобів криптографічного захисту інформації	
І. Загальні положення	
1. Це Положення визначає вимоги до порядку розроблення, виробництва та експлуатації засобів криптографічного захисту державних інформаційних ресурсів або інформації, вимога щодо захисту якої встановлена законом.	1. Це Положення визначає вимоги до порядку розроблення, виробництва та експлуатації засобів криптографічного захисту державних інформаційних ресурсів або інформації, вимога щодо захисту якої встановлена законом, **засобів удосконаленого електронного підпису чи печатки, засобів кваліфікованого електронного підпису чи печатки, засобів, спеціально призначених для розроблення, дослідження, виробництва та випробування засобів криптографічного захисту інформації (далі – засоби КЗІ).**
Особливості розроблення, виготовлення, уведення в експлуатацію та експлуатації засобів криптографічного захисту інформації **(далі - КЗІ)**, що становить державну таємницю, та службової інформації визначаються відповідно до чинного законодавства.	Особливості розроблення, виготовлення, уведення в експлуатацію та експлуатації **засобів КЗІ, призначених для криптографічного захисту інформації,** що становить державну таємницю, та службової інформації визначаються відповідно до чинного законодавства.
Розроблення засобів КЗІ, що фінансується за рахунок коштів Державного бюджету України, погоджується з Адміністрацією Державної служби спеціального зв'язку та захисту інформації України (далі - Адміністрація Держспецзв'язку).	Розроблення засобів КЗІ, що фінансується за рахунок коштів Державного бюджету України, погоджується з Адміністрацією Державної служби спеціального зв'язку та захисту інформації України (далі - Адміністрація Держспецзв'язку).
Національний банк України може розробляти засоби КЗІ, призначені виключно для забезпечення власних потреб та потреб банківської системи України, без погодження з Адміністрацією Держспецзв'язку.	Національний банк України може розробляти засоби КЗІ, призначені виключно для забезпечення власних потреб та потреб банківської системи України, без погодження з Адміністрацією Держспецзв'язку.
2. Вимоги цього Положення обов'язкові для виконання державними	2. Вимоги цього Положення обов'язкові для виконання державними

органами, підприємствами, установами і організаціями незалежно від форм власності (далі - організації), діяльність яких пов'язана з розробленням, виробництвом, сертифікаційними випробуваннями (експертними роботами) та експлуатацією засобів КЗІ, **надійних засобів електронного цифрового підпису та засобів, спеціально призначених для розроблення, дослідження, виробництва та випробування засобів КЗІ.** **…**	органами, підприємствами, установами і організаціями незалежно від форм власності (далі - організації), діяльність яких пов'язана з розробленням, виробництвом, сертифікаційними випробуваннями (експертними роботами) та експлуатацією засобів КЗІ. **…**
4. У цьому Положенні використовуються такі терміни: … криптографічне перетворення інформації - перетворення інформації з використанням ключових даних з метою приховування (відновлення) змісту інформації, підтвердження її справжності, цілісності, авторства, дати створення тощо; … сертифікаційні випробування - випробування засобів КЗІ, що проводяться з метою встановлення відповідності їх характеристик та властивостей вимогам **нормативних документів у сфері КЗІ**; … Інші терміни, використані в цьому Положенні, відповідають термінам, визначеним у нормативно-правових актах у **сфері криптографічного захисту інформації та у сфері електронного цифрового підпису**.	4. У цьому Положенні використовуються такі терміни: … криптографічне перетворення інформації **(далі – криптоперетворення)** – перетворення інформації з використанням **криптографічних алгоритмів та** ключових даних з метою приховування (відновлення) змісту інформації, підтвердження її справжності, цілісності, авторства, дати створення тощо; … сертифікаційні випробування - випробування засобів КЗІ, що проводяться з метою встановлення відповідності їх характеристик та властивостей вимогам **законодавства та нормативних документів у сферах захисту інформації та інформаційної безпеки**; … Інші терміни, використані в цьому Положенні, відповідають термінам, визначеним у нормативно-правових актах у **сферах захисту інформації та електронних довірчих послуг.**
5. Залежно від способу реалізації розрізняють такі типи засобів КЗІ: … **засоби захисту від нав'язування неправдивої інформації або захисту від несанкціонованої модифікації, що реалізовують алгоритми криптографічного перетворення інформації (далі - криптоалгоритми), у тому числі засоби імітозахисту та електронного цифрового підпису** (далі - засоби категорії «П»);	5. Залежно від способу реалізації розрізняють такі типи засобів КЗІ: … **засоби, що реалізують криптоперетворення та/або механізми імітозахисту, та призначені для забезпечення захисту (підтвердження) хоча б однієї з таких властивостей інформації: справжності (авторства), цілісності, неспростовності, дати створення** (далі - засоби категорії «П»);

8. Роботи щодо засобів КЗІ виконують організації, які мають ліцензію на право провадження господарської діяльності з надання послуг у галузі криптографічного захисту інформації (крім **послуг електронного цифрового підпису)** та технічного захисту інформації, за переліком, що визначається Кабінетом Міністрів України.	8. Роботи щодо засобів КЗІ виконують організації, які мають ліцензію на право провадження господарської діяльності з надання послуг у галузі криптографічного захисту інформації (крім **електронних довірчих послуг)** та технічного захисту інформації, за переліком, що визначається Кабінетом Міністрів України.
9. Суб'єкти, які здійснюють розроблення, виробництво та експлуатацію засобів КЗІ, визначають режим доступу до інформації про ці засоби, установлюють і підтримують відповідний режим безпеки з урахуванням вимог замовника та відповідно до нормативно-правових актів у **сфері КЗІ.**	9. Суб'єкти, які здійснюють розроблення, виробництво та експлуатацію засобів КЗІ, визначають режим доступу до інформації про ці засоби, установлюють і підтримують відповідний режим безпеки з урахуванням вимог замовника та відповідно до нормативно-правових актів у **сферах захисту інформації та інформаційної безпеки**;
II. Розроблення засобів КЗІ	
1. Розроблення засобів КЗІ здійснюється відповідно до вимог нормативно-правових актів і національних стандартів **у сфері КЗІ**, а **також нормативних документів** з питань розроблення та поставлення продукції на виробництво.	1. Розроблення засобів КЗІ здійснюється відповідно до вимог нормативно-правових актів у **сферах захисту інформації та інформаційної безпеки**, розроблення та поставлення продукції на виробництво.
10. До ТЗ на ДКР з розроблення нового **типу** або модернізації існуючого зразка засобу КЗІ вносяться: … **Вимоги безпеки для криптографічних модулів, а також щодо перевіряння криптографічних модулів визначаються національними стандартами.** **…** **Вимоги до форматів даних та протоколів засобів КЗІ, призначених для застосування в системах електронного документообігу з використанням посилених сертифікатів відкритих ключів електронного цифрового підпису, визначаються Міністерством юстиції України та Адміністрацією Держспецзв'язку.**	10. До ТЗ на ДКР з розроблення нового або модернізації існуючого зразка засобу КЗІ вносяться: … - **Вимоги до засобів кваліфікованого електронного підпису чи печатки, визначаються Вимогами у сфері електронних довірчих послуг, затвердженими постановою Кабінету Міністрів України від 7 листопада 2018 р. № 992, наказами Міністерства юстиції України та Адміністрації Держспецзв'язку.**
12. … У цих методиках повинні наводитися методи та способи управління ключовими даними і порядок їх використання відповідно до обраного криптографічного алгоритму, види та кількість ключів, періодичність	12. … У цих методиках повинні наводитися методи та способи управління ключовими даними і порядок їх використання відповідно до обраного криптографічного алгоритму, види та кількість ключів, періодичність їх

їх зміни, протоколи розподілу ключів, а також повний опис криптографічних функцій, що застосовані для генерації ключових даних та управління ключами, якщо вони відрізняються від тих криптоалгоритмів та криптопротоколів, що зазначені в абзаці першому цього пункту. Можливість погодження цих методик визначається за результатами державної експертизи у **сфері КЗІ**.	зміни, протоколи розподілу ключів, а також повний опис криптографічних функцій, що застосовані для генерації ключових даних та управління ключами, якщо вони відрізняються від тих криптоалгоритмів та криптопротоколів, що зазначені в абзаці першому цього пункту. Можливість погодження цих методик визначається за результатами державної експертизи у **сфері криптографічного захисту інформації (далі – КЗІ)**.
15. На етапі ескізно-технічного проектування здійснюються опрацювання та **практична реалізація** функцій захисту згідно з вимогами до засобів КЗІ. При цьому основна увага при проектуванні засобу КЗІ приділяється вузлам оброблення критичної інформації, у тому числі: уведення та оброблення ключових даних; оброблення вхідної та вихідної інформації; шифрування інформації; формування/перевіряння **електронного цифрового підпису**; генераторів випадкових (псевдовипадкових) послідовностей, які використовуються для формування ключів, векторів ініціалізації тощо; самотестування; системи сигналізації при несанкціонованому доступі до засобу КЗІ, зміні параметрів навколишнього середовища, електроживлення тощо.	15. На етапі ескізно-технічного проектування здійснюються опрацювання та **реалізація функцій захисту відповідних проєктних рішень** згідно з вимогами до засобів КЗІ. При цьому основна увага при проектуванні засобу КЗІ приділяється вузлам оброблення критичної інформації, у тому числі: уведення та оброблення ключових даних; оброблення вхідної та вихідної інформації; шифрування інформації; формування/перевіряння **цифрового підпису**; генераторів випадкових (псевдовипадкових) послідовностей, які використовуються для формування ключів, векторів ініціалізації тощо; самотестування; системи сигналізації при несанкціонованому доступі до засобу КЗІ, зміні параметрів навколишнього середовища, електроживлення тощо.
IV. Експлуатація засобів КЗІ	
1. Для криптографічного захисту державних інформаційних ресурсів або інформації, вимога щодо захисту якої встановлена законом, використовуються засоби КЗІ, які мають сертифікат відповідності або позитивний експертний висновок за результатами державної експертизи у сфері КЗІ, а суб'єкти, що їх використовують, мають на це права. Сертифікація засобів КЗІ та державна експертиза у сфері	1. Для криптографічного захисту державних інформаційних ресурсів або інформації, вимога щодо захисту якої встановлена законом, використовуються засоби КЗІ, які мають **документ про відповідність** або позитивний експертний висновок за результатами державної експертизи у сфері КЗІ, **що підтверджують клас засобу КЗІ (рівень гарантій) та реалізовані методи захисту**, а суб'єкти, що їх використовують, мають на це права. **Оцінка відповідності та** державна експертиза у сфері криптографічного захисту інформації проводяться в порядку,

криптографічного захисту інформації проводяться в порядку, визначеному відповідними нормативно-правовими актами.	визначеному відповідними нормативно-правовими актами.
3. Кожний екземпляр засобів КЗІ береться на облік в організації з дати їх отримання. … Облік засобів КЗІ та носіїв ключової інформації до них в організації забезпечується відповідальними особами, визначеними відповідними актами організаційно-розпорядчого характеру цієї організації. Збереження засобів КЗІ, носіїв ключової інформації забезпечується відповідальною особою, функціональними обов'язками якої це визначено. Особливості обліку засобів КЗІ, зазначених в пункті 3 розділу I цього Положення, визначаються Національним банком України.	3. Кожний екземпляр засобів КЗІ береться на облік в організації з дати їх отримання. … Облік засобів КЗІ та носіїв ключової інформації до них в організації забезпечується відповідальними особами, визначеними відповідними актами організаційно-розпорядчого характеру цієї організації. Збереження засобів КЗІ, носіїв ключової інформації забезпечується відповідальною особою, функціональними обов'язками якої це визначено. Особливості обліку засобів КЗІ, зазначених в пункті 3 розділу I цього Положення, визначаються Національним банком України. **Особливості обліку засобів удосконаленого електронного підпису чи печатки, засобів кваліфікованого електронного підпису чи печатки та носіїв ключової інформації до них визначаються нормативно-правовими актами у сфері електронних довірчих послуг.**
Наказ Адміністрації Держспецзв'язку від 23.06.2008 № 100 «Про затвердження Положення про державну експертизу в сфері криптографічного захисту інформації», зареєстрований в Мін'юсті 16.07.2008 за № 651/15342 (зі змінами)	
Положення про державну експертизу в сфері криптографічного захисту інформації	
I. Загальні положення	
1.3. Використані в цьому Положенні терміни вживаються в такому значенні: … Інші терміни вживаються у значенні, наведеному в Законах України «Про Державну службу спеціального зв'язку та захисту інформації України», «Про захист інформації в інформаційно-телекомунікаційних системах», Положенні про порядок здійснення криптографічного захисту інформації в Україні, затвердженому Указом Президента України від 22 травня 1998 року № 505, **Правилах**	1.3. Використані в цьому Положенні терміни вживаються в такому значенні: … Інші терміни вживаються у значенні, наведеному в Законах України «Про Державну службу спеціального зв'язку та захисту інформації України», «Про захист інформації в інформаційно-телекомунікаційних системах», **«Про електронні довірчі послуги»**, Положенні про порядок здійснення криптографічного захисту інформації в Україні, затвердженому Указом Президента України від 22

посиленої сертифікації, затверджених наказом Департаменту спеціальних телекомунікаційних систем та захисту інформації Служби безпеки України від 13 січня 2005 року № 3, зареєстрованих у Міністерстві юстиції України 27 січня 2005 року за № 104/10384, Положенні про порядок розроблення, виробництва та експлуатації засобів криптографічного захисту інформації, затвердженому наказом Адміністрації Державної служби спеціального зв'язку та захисту інформації України від 20 липня 2007 року № 141, зареєстрованому у Міністерстві юстиції України 30 липня 2007 року за № 862/14129 (із змінами).	травня 1998 року № 505, Положенні про порядок розроблення, виробництва та експлуатації засобів криптографічного захисту інформації, затвердженому наказом Адміністрації Державної служби спеціального зв'язку та захисту інформації України від 20 липня 2007 року № 141, зареєстрованому у Міністерстві юстиції України 30 липня 2007 року за № 862/14129 (із змінами).
1.5. Об'єктами експертизи є: засоби та методи, призначені для розробки, дослідження, виробництва та випробувань засобів КЗІ; звіти про наукові дослідження і розробки, результати тематичних досліджень, інші результати наукової та науково-технічної діяльності у сфері КЗІ; криптографічні алгоритми та протоколи; алгоритми, протоколи, засоби та системи генерації, тестування та розподілу ключових даних; **криптографічні системи, засоби та обладнання КЗІ, програмно-технічні комплекси центрів сертифікації ключів, надійні засоби електронного цифрового підпису (далі - криптографічні засоби);** положення державних і міждержавних програм та проектів державного значення в частині, що стосується КЗІ.	1.5. Об'єктами експертизи є: засоби та методи, призначені для розробки, дослідження, виробництва та випробувань засобів КЗІ; звіти про наукові дослідження і розробки, результати тематичних досліджень, інші результати наукової та науково-технічної діяльності у сфері КЗІ; криптографічні алгоритми та протоколи; алгоритми, протоколи, засоби та системи генерації, тестування та розподілу ключових даних; **криптосистеми, засоби та обладнання КЗІ (далі - криптографічні засоби);** положення державних і міждержавних програм та проектів державного значення в частині, що стосується КЗІ.
1.6. Експертиза є обов'язковою або добровільною. Обов'язковій експертизі підлягають: … криптосистеми, засоби й обладнання криптографічного захисту державних інформаційних ресурсів або інформації, вимога щодо захисту якої встановлена законом, програмно-технічні комплекси центрів сертифікації ключів, які передбачають акредитацію, надійні	1.6. Експертиза є обов'язковою або добровільною. Обов'язковій експертизі підлягають: … криптосистеми, засоби й обладнання криптографічного захисту державних інформаційних ресурсів або інформації, вимога щодо захисту якої встановлена законом, **криптосистеми, що використовуються для надання кваліфікованих електронних довірчих послуг, або в схемах**

засоби електронного цифрового підпису; …	**електронної ідентифікації, засоби удосконаленого електронного підпису чи печатки, засоби кваліфікованого електронного підпису чи печатки;** **засоби, що реалізують криптоперетворення та/або механізми імітозахисту, та використовуються в системах зв'язку, управління та озброєння;** **засоби обробки та передачі державних інформаційних ресурсів або інформації, вимога щодо захисту якої встановлена законом, які реалізують функції криптографічного захисту інформації.**
II. Порядок організації та проведення експертизи	
2.1.1. Для проведення експертизи таких об'єктів, як: засоби, призначені для розробки, дослідження, виробництва та випробувань засобів КЗІ; засоби та системи генерації, тестування і розподілу ключових даних; криптографічні системи, засоби та обладнання КЗІ, **програмно-технічні комплекси центрів сертифікації ключів, які передбачають акредитацію, надійні засоби електронного цифрового підпису** …	2.1.1. Для проведення експертизи таких об'єктів, як: засоби, призначені для розробки, дослідження, виробництва та випробувань засобів КЗІ; засоби та системи генерації, тестування і розподілу ключових даних; криптографічні системи, засоби та обладнання КЗІ, **засоби удосконаленого електронного підпису чи печатки, засоби кваліфікованого електронного підпису чи печатки;** …
Додаток 2 **ПЕРЕЛІК** **документів та матеріалів, необхідних для проведення експертизи криптографічних засобів вітчизняного виробництва**	
8. Технічна документація на апаратні (апаратно-програмні) компоненти: технічні завдання (згідно з ДСТУ 3973-2000 Система розроблення та поставлення продукції на виробництво. Правила виконання науково-дослідних робіт. Загальні положення, ДСТУ 3974-2000 Система розроблення та поставлення продукції на виробництво. Правила виконання дослідно-конструкторських робіт. Загальні положення) **та технічні умови (згідно з ДСТУ 1.3:2004 "Національна**	8. Технічна документація на апаратні (апаратно-програмні) компоненти: технічні завдання (згідно з ДСТУ 3973-2000 Система розроблення та поставлення продукції на виробництво. Правила виконання науково-дослідних робіт. Загальні положення, ДСТУ 3974-2000 Система розроблення та поставлення продукції на виробництво. Правила виконання дослідно-конструкторських робіт. Загальні положення);

стандартизація. Правила побудови, викладання, оформлення, погодження, прийняття та позначення технічних умов, ДСТУ - Н 4486:2005 Система конструкторської документації. Настанови щодо типової побудови технічних умов, ГОСТ 2.114-95 "Единая система конструкторской документации. Технические условия"); …	…
9. Програмна документація на програмні компоненти: технічне завдання **(згідно з ГОСТ 19.201-78 "Единая система программной документации. Техническое задание. Требования к содержанию и оформлению");** **технічні умови (згідно з ДСТУ 1.3:2004 Національна стандартизація. Правила побудови, викладання, оформлення, погодження, прийняття та позначення технічних умов (за потреби);** специфікація **(згідно з ГОСТ 19.202-78 "Единая система программной документации. Спецификация. Требования к содержанию и оформлению");** тексти програм **(згідно з ГОСТ 19.401-78 "Единая система программной документации. Текст программы. Требования к содержанию и оформлению");** описи програм **(згідно з ГОСТ 19.402-78 "Единая система программной документации. Описание программы");** програма та методика випробувань **(згідно з ГОСТ 19.301-79 "Единая система программной документации. Программа и методика испытаний. Требования к содержанию и оформлению");** настанова системного програміста **(згідно з ГОСТ 19.503-79 "Единая система программной документации. Руководство системного программиста. Требования к содержанию и оформлению");** настанова програміста **(згідно з ГОСТ 19.504-79 "Единая система программной документации. Руководство программиста.**	9. Програмна документація на програмні компоненти: технічне завдання; технічні умови; специфікація; тексти програм; описи програм; програма та методика випробувань; настанова системного програміста; настанова програміста;

Требования к содержанию и оформлению"); настанова оператора **(згідно з ГОСТ 19.505-79 "Единая система программной документации. Руководство оператора. Требования к содержанию и оформлению").**	настанова оператора.
Наказ Адміністрації Держспецзв'язку від 18.12.2012 № 739 «Про затвердження вимог до форматів криптографічних повідомлень», зареєстрований в Міністерстві юстиції України 14.01.2013 за № 108/22640 (зі змінами)	
2. Установити, що акредитовані центри сертифікації ключів, замовники, розробники, виробники та організації, які експлуатують засоби криптографічного захисту інформації та надійні засоби електронного цифрового підпису в системах електронного документообігу, забезпечують застосування положень Вимог з 01 січня 2014 року.	**2. Установити, що державні органи при електронній взаємодії, що здійснюється з використанням кваліфікованих електронних довірчих послуг, при здійсненні обміну електронних даних конфіденційного характеру через глобальні мережі передачі даних, забезпечують конфіденційність таких даних з використанням засобів криптографічного захисту інформації та сертифікатів шифрування, що відповідають Вимогам.**
3. Установити, що акредитовані центри сертифікації ключів забезпечують обслуговування посилених сертифікатів відкритих ключів, сформованих до дати набрання чинності Вимогами, та їх використання у надійних засобах електронного цифрового підпису та засобах криптографічного захисту інформації як сертифікати шифрування до закінчення строку чинності посилених сертифікатів відкритих ключів за умови відповідності параметрів криптографічного алгоритму відповідної ключової пари вимогам, наведеним у наказі Міністерства юстиції України, Адміністрації Державної служби спеціального зв'язку та захисту інформації України від 20 серпня 2012 року № 1236/5/453 "Про затвердження вимог до форматів, структури та протоколів, що реалізуються у надійних засобах електронного цифрового підпису", зареєстрованому в Міністерстві юстиції України 20 серпня 2012 року за № 1398/21710.	**3 Установити, що кваліфіковані надавачі електронних довірчих послуг мають право надавати послуги з обслуговування сертифікатів шифрування, та у разі фактичного їх надання інформують про це Адміністрацію Держспецзв'язку.**
4. Установити, що надійні засоби електронного цифрового підпису та криптографічного захисту інформації, створювані відповідно до цих Вимог, забезпечують розшифрування даних, шифрування яких здійснювалося до дати набрання чинності Вимогами.	-

5. Директору Департаменту криптографічного захисту інформації Адміністрації Державної служби спеціального зв'язку та захисту інформації України в установленому порядку забезпечити подання цього наказу на державну реєстрацію до Міністерства юстиції України.	**4.** Директору Департаменту криптографічного захисту інформації Адміністрації Державної служби спеціального зв'язку та захисту інформації України в установленому порядку забезпечити подання цього наказу на державну реєстрацію до Міністерства юстиції України.
6. Цей наказ набирає чинності з дня його офіційного опублікування.	**5.** Цей наказ набирає чинності з дня його офіційного опублікування.
7. Контроль за виконанням цього наказу покласти на першого заступника Голови Державної служби спеціального зв'язку та захисту інформації України.	**6.** Контроль за виконанням цього наказу покласти на першого заступника Голови Державної служби спеціального зв'язку та захисту інформації України.
Вимоги до форматів криптографічних повідомлень	
I. Загальні положення	
1.1. Ці Вимоги визначають синтаксис (формат представлення) криптографічних повідомлень (зашифрованих даних) в електронній формі, а також протоколи узгодження ключів для засобів криптографічного захисту інформації (далі – КЗІ) **та надійних засобів електронного цифрового підпису (далі – ЕЦП).**	1.1. Ці Вимоги визначають синтаксис (формат представлення) криптографічних повідомлень (зашифрованих даних) в електронній формі, а також протоколи узгодження ключів для засобів криптографічного захисту інформації (далі – КЗІ).
1.2. Положення цих Вимог є обов'язковими для засобів КЗІ **та надійних засобів ЕЦП**, призначених для забезпечення конфіденційності інформації з використанням сертифіката шифрування. Правильність реалізації у засобах КЗІ **та надійних засобах ЕЦП наведених у цих Вимогах форматів і протоколів повинна бути підтверджена сертифікатом відповідності або** позитивним експертним висновком за результатами державної експертизи у сфері криптографічного захисту інформації.	1.2. Положення цих Вимог є обов'язковими для засобів КЗІ, призначених для забезпечення конфіденційності інформації з використанням сертифіката шифрування. Правильність реалізації у засобах КЗІ **цих Вимог повинна бути підтверджена документом про відповідність або** позитивним експертним висновком за результатами державної експертизи у сфері **КЗІ**. **Оцінка відповідності та державна експертиза у сфері КЗІ проводяться в порядку, визначеному відповідними нормативно-правовими актами.**
1.3. У цих Вимогах терміни вживаються у таких значеннях: дані – повідомлення або частина повідомлення, яке не обробляють чи не змінюють у процесі обробки; механізм узгодження ключа – статичний (Static-Static mode) або динамічний (Ephemeral-Static mode) механізм узгодження ключа, що визначений у цих Вимогах; повідомлення "захищені дані" – повідомлення, що містить	1.3. У цих Вимогах терміни вживаються у таких значеннях: дані – повідомлення або частина повідомлення, яке не обробляють чи не змінюють у процесі обробки; механізм узгодження ключа – статичний (Static-Static mode) або динамічний (Ephemeral-Static mode) механізм узгодження ключа, що визначений у цих Вимогах; повідомлення "захищені дані" – повідомлення, що містить цифровий

цифровий конверт; протокол узгодження ключа – протокол Діффі-Геллмана обчислення ключа шифрування ключа (КШК) **у циклічній групі поля або** в групі точок еліптичної кривої; симетричний ключ сеансу або ключ шифрування даних (КШД) – ключ сеансу, на якому здійснюється шифрування даних за визначеним у цих Вимогах алгоритмом криптографічного перетворення; узгоджений ключ (“key agreement”) або ключ шифрування ключа (КШК) – симетричний ключ, на якому здійснюється шифрування симетричного ключа сеансу; цифровий конверт (“enveloped-data”) – зашифровані дані типу “дані” (“data”) або “підписані дані” (“signed-data”) разом із зашифрованим симетричним ключем. **Інші терміни вживаються у значеннях, наведених у Законі України “Про електронний цифровий підпис”, Порядку акредитації центру сертифікації ключів, затвердженому постановою Кабінету Міністрів України від 13 липня 2004 року № 903, Правилах посиленої сертифікації, затверджених наказом Департаменту спеціальних телекомунікаційних систем та захисту інформації Служби безпеки України від 13 січня 2005 року № 3, зареєстрованих у Міністерстві юстиції України 27 січня 2005 року за № 104/10384 (із змінами).**	конверт; протокол узгодження ключа – протокол Діффі-Геллмана обчислення ключа шифрування ключа (КШК) в групі точок еліптичної кривої; **сертифікат шифрування – сертифікат відкритого ключа виданий надавачем електронних довірчих послуг та призначений для використання у протоколі узгодження ключа;** симетричний ключ сеансу або ключ шифрування даних (КШД) – ключ сеансу, на якому здійснюється шифрування даних за визначеним у цих Вимогах алгоритмом криптографічного перетворення; узгоджений ключ (“key agreement”) або ключ шифрування ключа (КШК) – симетричний ключ, на якому здійснюється шифрування симетричного ключа сеансу; цифровий конверт (“enveloped-data”) – зашифровані дані типу “дані” (“data”) або “підписані дані” (“signed-data”) разом із зашифрованим симетричним ключем. **Інші терміни вживаються у значеннях, наведених у Законі України “Про електронні довірчі послуги” та нормативно-правових актах у сфері електронних довірчих послуг.**
1.4. У цих Вимогах скорочення мають такі значення: CMS – синтаксис криптографічного повідомлення (Cryptographic Message Syntax); **DH – протокол узгодження ключів Діффі-Геллмана (Diffie-Hellman), що базується на криптографічних перетвореннях у полі Галуа; може використовуватися також позначення FFC DH (Finite Field Cryptography Diffie-Hellman);** ECDH – протокол Діффі-Геллмана (Diffie-Hellman), що базується на	1.4. У цих Вимогах скорочення мають такі значення: CMS – синтаксис криптографічного повідомлення (Cryptographic Message Syntax); ECDH – протокол **узгодження ключів** Діффі-Геллмана (Diffie-

криптографічних перетвореннях у групі точок еліптичної кривої; може використовуватися також позначення ECC DH (Elliptic Curve Cryptography Diffie-Hellman); ДКЕ – довгостроковий ключовий елемент.	Hellman), що базується на криптографічних перетвореннях у групі точок еліптичної кривої; може використовуватися також позначення ECC DH (Elliptic Curve Cryptography Diffie-Hellman); ДКЕ – довгостроковий ключовий елемент.
1.5. Ці Вимоги базуються на рекомендаціях Комітету із інженерних питань Інтернету RFC 3370 "Cryptographic Message Syntax (CMS) Algorithms", August 2002 (далі – RFC 3370); RFC 3852 "Cryptographic Message Syntax (CMS)", July 2004 (далі – RFC 3852); RFC 5652 "Cryptographic Message Syntax (CMS)", September 2009 (далі – RFC 5652), національному стандарті України ДСТУ ISO/IEC 11770-3:2015 "Інформаційні технології. Методи захисту. Керування ключами. Частина 3. Механізми з використанням асиметричних методів" (далі – ДСТУ ISO/IEC 11770-3:2015) та встановлюють особливості застосування в них криптографічних алгоритмів, визначених стандартами **ГОСТ 34.310-95 "Информационная технология. Криптографическая защита информации. Процессы выработки и проверки электронной цифровой подписи на базе ассиметричного криптографического алгоритма" (далі – ГОСТ 34.310-95)**, ДСТУ 4145-2002 "Інформаційні технології. Криптографічний захист інформації. Цифровий підпис, що ґрунтується на еліптичних кривих. Формування та перевіряння" (далі – ДСТУ 4145-2002), ДСТУ ГОСТ 28147:2009 "Системы обработки информации. Защита криптографическая. Алгоритмы криптографического преобразования" (далі – ДСТУ ГОСТ 28147:2009), ДСТУ 7624:2014 "Інформаційні технології. Криптографічний захист інформації. Алгоритм симетричного блокового перетворення" (далі – ДСТУ 7624:2014), ДСТУ ISO/IEC 10118-3:2005 "Інформаційні технології. Методи захисту. Геш-функції. Частина 3. Спеціалізовані геш-функції" (далі – ДСТУ ISO/IEC 10118-3:2005). Під час застосування міжнародних алгоритмів **ЕЦП** застосовуються вимоги RFC 3370, RFC 3852, RFC 5652, ISO/IEC 11770-3, ISO/IEC 10118-3.	1.5. Ці Вимоги базуються на рекомендаціях Комітету із інженерних питань Інтернету RFC 3370 "Cryptographic Message Syntax (CMS) Algorithms", August 2002 (далі – RFC 3370); RFC 3852 "Cryptographic Message Syntax (CMS)", July 2004 (далі – RFC 3852); RFC 5652 "Cryptographic Message Syntax (CMS)", September 2009 (далі – RFC 5652), національному стандарті України ДСТУ ISO/IEC 11770-3:2015 "Інформаційні технології. Методи захисту. Керування ключами. Частина 3. Механізми з використанням асиметричних методів" (далі – ДСТУ ISO/IEC 11770-3:2015) та встановлюють особливості застосування в них криптографічних алгоритмів, визначених стандартами ДСТУ 4145-2002 "Інформаційні технології. Криптографічний захист інформації. Цифровий підпис, що ґрунтується на еліптичних кривих. Формування та перевіряння" (далі – ДСТУ 4145-2002), ДСТУ ГОСТ 28147:2009 "Системы обработки информации. Защита криптографическая. Алгоритмы криптографического преобразования" (далі – ДСТУ ГОСТ 28147:2009), ДСТУ 7624:2014 "Інформаційні технології. Криптографічний захист інформації. Алгоритм симетричного блокового перетворення" (далі – ДСТУ 7624:2014), ДСТУ ISO/IEC 10118-3:2005 "Інформаційні технології. Методи захисту. Геш-функції. Частина 3. Спеціалізовані геш-функції" (далі – ДСТУ ISO/IEC 10118-3:2005). Під час застосування міжнародних алгоритмів **цифрового підпису** застосовуються вимоги RFC 3370, RFC 3852, RFC 5652, ISO/IEC 11770-3, ISO/IEC 10118-3.
1.8. Ці Вимоги розроблено з урахуванням Інструкції про порядок постачання і використання ключів до засобів криптографічного захисту інформації, затвердженої наказом Адміністрації Державної служби	1.8. Ці Вимоги розроблено з урахуванням Інструкції про порядок постачання і використання ключів до засобів криптографічного захисту інформації, затвердженої наказом Адміністрації Державної служби

спеціального зв'язку та захисту інформації України від 12 червня 2007 року № 114, зареєстрованої в Міністерстві юстиції України 25 червня 2007 року за № 729/13996 (далі – Інструкція № 114), **Вимог до формату посиленого сертифіката відкритого ключа, затверджених наказом Міністерства юстиції України, Адміністрації Державної служби спеціального зв'язку та захисту інформації України від 20 серпня 2012 року № 1236/5/453, зареєстрованих у Міністерстві юстиції України 20 серпня 2012 року за № 1398/21710 (далі – Вимоги до формату посиленого сертифіката відкритого ключа), Вимог до формату списку відкликаних сертифікатів, затверджених наказом Міністерства юстиції України, Адміністрації Державної служби спеціального зв'язку та захисту інформації України від 20 серпня 2012 року № 1236/5/453, зареєстрованих у Міністерстві юстиції України 20 серпня 2012 року за № 1400/21712 (далі – Вимоги до формату списку відкликаних сертифікатів), Вимог до формату підписаних даних, затверджених наказом Міністерства юстиції України, Адміністрації Державної служби спеціального зв'язку та захисту інформації України від 20 серпня 2012 року № 1236/5/453, зареєстрованих у Міністерстві юстиції України 20 серпня 2012 року за № 1401/21713 (далі – Вимоги до формату підписаних даних).**	спеціального зв'язку та захисту інформації України від 12 червня 2007 року № 114, зареєстрованої в Міністерстві юстиції України 25 червня 2007 року за № 729/13996 (далі – Інструкція № 114), **Вимог до електронних довірчих послуг, затверджених постановою Кабінету Міністрів України від 07 листопада 2018 року № 992 (далі – Вимоги до електронних довірчих послуг).**
1.9. У цих Вимогах повинні застосовуватися криптографічні алгоритми, що застосовуються у Вимогах до формату посиленого сертифіката відкритого ключа. Режими роботи криптографічних алгоритмів встановлюються цими Вимогами.	-
II. Типи повідомлень	
2.2. Тип повідомлення "ContentInfo" подано в нотації ASN.1, яка визначена у ДСТУ ISO/IEC 8824-1:**2009** "Інформаційні технології. Нотація абстрактного синтаксису 1 (ASN.1). Частина 1. Специфікація базової нотації", ДСТУ ISO/IEC 8824-2:**2009** "Інформаційні технології. Нотація абстрактного синтаксису 1 (ASN.1). Частина 2. Специфікація інформаційного об'єкта", ДСТУ ISO/IEC 8824-3:**2009** "Інформаційні технології. Нотація абстрактного синтаксису 1 (ASN.1). Частина 3. Специфікація обмежень", ДСТУ ISO/IEC 8824-4:**2009** "Інформаційні технології. Нотація абстрактного синтаксису 1 (ASN.1). Частина 4.	Тип повідомлення «ContentInfo» подано в нотації ASN.1, яка визначена ДСТУ ISO/IEC 8824-1:**2017 (ISO/IEC 8824-1:2015, IDT)** «Інформаційні технології. Нотація абстрактного синтаксису 1 (ASN.1). Частина 1. Специфікація базової нотації», ДСТУ ISO/IEC 8824-2:**2017 (ISO/IEC 8824-2:2015, IDT)** «Інформаційні технології. Нотація абстрактного синтаксису 1 (ASN.1). Частина 2. Специфікація інформаційного об'єкта», ДСТУ ISO/IEC 8824-3:**2008 (ISO/IEC 8824-3:2002, IDT)** «Інформаційні технології. Нотація абстрактного синтаксису 1 (ASN.1). Частина 3. Специфікація обмежень», ДСТУ

Параметризація специфікацій ASN.1" (далі - ISO/IEC 8824).	ISO/IEC 8824-4:**2017 (ISO/IEC 8824-4:2015, IDT)** «Інформаційні технології. Нотація абстрактного синтаксису 1 (ASN.1). Частина 4. Параметризація специфікацій ASN.1»
2.7. Формат повідомлення "підписані дані" ("signed-data") встановлюється Вимогами до **формату підписаних даних.** На тип "signed-data" вказує такий об'єктний ідентифікатор: id-signedData OBJECT IDENTIFIER ::= { iso(1) member-body(2) us(840) rsadsi(113549) pkcs(1) pkcs7(7) 2 }.	2.7. Формат повідомлення "підписані дані" ("signed-data") встановлюється Вимогами до **електронних довірчих послуг**. На тип "signed-data" вказує такий об'єктний ідентифікатор: id-signedData OBJECT IDENTIFIER ::= { iso(1) member-body(2) us(840) rsadsi(113549) pkcs(1) pkcs7(7) 2 }.
III. Процедура формування та розкриття "захищених даних"	
3. Особливості формування повідомлення "захищені дані"	
3.2. При використанні криптографічних перетворень у циклічній групі поля та в групі точок еліптичної кривої застосовується статичний або динамічний механізм узгодження ключів.	**3.2. Для формування повідомлення "захищені дані" застосовується статичний або динамічний механізм узгодження ключів за протоколом Діффі-Геллмана**
3.2.1 Статичний механізм узгодження ключів ("Static-Static mode") – узгодження ключів за протоколом Діффі-Геллмана, за якого як відправник, так і одержувач мають статичну ключову пару, відкритий ключ якої засвідчено **в акредитованому центрі сертифікації ключів.** Статичний механізм узгодження ключів може використовуватися лише у випадку, коли параметри криптографічного алгоритму статичної ключової пари відправника еквівалентні параметрам криптографічного алгоритму статичної ключової пари одержувача. Якщо зазначені параметри не еквівалентні, повинен застосовуватися динамічний механізм узгодження ключів. При статичному механізмі узгодження ключа для формування узгодженого ключа відправник повинен використовувати особистий ключ відправника та відкритий ключ одержувача. Одержувач повинен використовувати особистий ключ одержувача та відкритий ключ відправника. Відкриті ключі відправника та одержувача обираються **із посилених сертифікатів відкритих ключів** (сертифікатів шифрування).	3.2.1 Статичний механізм узгодження ключів ("Static-Static mode") – узгодження ключів за протоколом Діффі-Геллмана, за якого як відправник, так і одержувач мають статичну ключову пару, **відкритий ключ якої засвідчено кваліфікованим надавачем електронних довірчих послуг.** Статичний механізм узгодження ключів може використовуватися лише у випадку, коли параметри криптографічного алгоритму статичної ключової пари відправника еквівалентні параметрам криптографічного алгоритму статичної ключової пари одержувача. Якщо зазначені параметри не еквівалентні, повинен застосовуватися динамічний механізм узгодження ключів. При статичному механізмі узгодження ключа для формування узгодженого ключа відправник повинен використовувати особистий ключ відправника та відкритий ключ одержувача. Одержувач повинен використовувати особистий ключ одержувача та відкритий ключ відправника. **Відкриті ключі відправника та одержувача обираються із сертифікатів шифрування.**
3.2.2. … **Протокол узгодження ключів Діффі-Геллмана в циклічній групі поля використовується для ключових пар (відправника та**	3.2.2. … -

одержувача), що відповідають ГОСТ 34.310-95 (але тільки за умови використання в режимі з довжиною модуля P 1024). …	…
IV. Представлення структури "захищені дані"	
3. Поля структури "EnvelopedData"	
3.2. Поле "originatorInfo" містить сертифікати відкритих ключів і списки відкликаних сертифікатів відправника. Поле є необов'язковим.	3.2. Поле "originatorInfo" містить **сертифікат шифрування** відправника **та додатково може містити пов'язані з ним кваліфіковані** сертифікати відкритих ключів і списки відкликаних сертифікатів. Поле є необов'язковим.
3.3.1. Поле "certs" – ланцюжок (chain) сертифікатів відправника, пов'язаний із статичним механізмом узгодження ключів, який було застосовано. Ланцюжок "certs" може містити лише **кінцевий сертифікат** відправника **або повний ланцюжок (chain) сертифікатів, достатній** для побудови шляху сертифікації від довіреного "кореня", **або може містити не повний ланцюжок (chain) сертифікатів, наприклад, кінцевий сертифікат відправника та сертифікат його центру сертифікації.** Сертифікати розміщуються в такому порядку: першим (з найменшим індексом) розміщується **сертифікат центру сертифікації** вищого рівня (кореневий **для повного ланцюга сертифікатів**), останнім (з найбільшим індексом) розміщується сертифікат відправника, який було застосовано для статичного механізму. **Наявність сертифіката відправника робить структуру захищених даних "самодостатньою" у тому розумінні, що дає змогу одержувачу розшифрувати повідомлення, використовуючи відкритий ключ відправника з його сертифіката, який міститься в полі "originatorInfo", без необхідності пошуку сертифіката відправника у сховищі сертифікатів.**	3.3.1. Поле "certs" містить **сертифікат шифрування** відправника та додатково може містити **пов'язані з ним кваліфіковані сертифікати відкритих ключів** для побудови шляху сертифікації від довіреного "кореня". Сертифікати розміщуються в такому порядку: першим (з найменшим індексом) розміщується **кваліфікований сертифікат відкритого ключа** вищого рівня (кореневий), останнім (з найбільшим індексом) розміщується **сертифікат шифрування** відправника, який було застосовано для статичного механізму.
3.4.1. Поле "crls" – набір списків відкликаних сертифікатів (CRL). Набір CRL містить інформацію, достатню для того, щоб визначити, чи є сертифікати в полі "certs" чинними. Послідовність розміщення CRL у полі "crls" повинна відповідати послідовності розміщення сертифікатів у наборі "certs". Наявність списків відкликання дає змогу одержувачу визначити чинність **сертифіката** відправника на момент формування захищених даних без необхідності звернення до зовнішніх джерел	3.4.1. Поле "crls" **містить** набір списків відкликаних сертифікатів (CRL). Набір CRL містить інформацію, достатню для того, щоб визначити, чи є сертифікати в полі "certs" чинними. Послідовність розміщення CRL у полі "crls" повинна відповідати послідовності розміщення сертифікатів у наборі "certs". Наявність списків **відкликаних сертифікатів** дає змогу одержувачу визначити чинність **сертифіката шифрування** відправника на момент формування

розміщення CRL.	захищених даних без необхідності звернення до зовнішніх джерел розміщення CRL.
3.7.4. Поля структури “KeyAgreeRecipientInfo”: … 3) ідентифікаційні дані відправника: під час застосування статичного механізму узгодження ключів Діффі-Геллмана як ідентифікатора відправника повинні використовуватися ім’я емітента сертифіката **(центру сертифікації)** та серійний номер сертифіката відкритого ключа відправника “issuerAndSerialNumber” або ідентифікатор відкритого ключа відправника “subjectKeyIdentifier”; під час застосування динамічного механізму узгодження ключів Діффі-Геллмана як ідентифікаційних даних відправника застосовується його відкритий сеансовий ключ (маркер), що генерується відправником та міститься в полі “originatorKey”; **під час застосування динамічного механізму узгодження ключів у циклічній групі поля поле “algorithm” в “originatorKey” повинно мати таке значення:** **Gost34310WithGost34311 OBJECT IDENTIFIER ::= { iso(1) member-body(2) Ukraine(804) root (2) security(1) cryptography(1) ua-pki (1) alg(1) asym(3) Gost34310WithGost34311(2)}.** **Відповідно до RFC 3370 параметрів алгоритму поля “algorithm” в “originatorKey” не повинно бути.** **Поле “originatorKey publicKey” повинно містити відкритий ключ відправника (маркер), що має такий формат:** **PublicKey:: = INTEGER, що інкапсулюється в BIT STRING.** **Відкритий ключ ГОСТ 34.310-95 кодується як ціле відповідно до Вимог до формату посиленого сертифіката відкритого ключа.** Під час застосування динамічного механізму узгодження ключів у групі точок еліптичної кривої поле “algorithm” поля “originatorKey” для алгоритму цифрового підпису ДСТУ 4145-2002 може мати такі значення: …	3.7.4. Поля структури “KeyAgreeRecipientInfo”: … 3) ідентифікаційні дані відправника: під час застосування статичного механізму узгодження ключів Діффі-Геллмана як ідентифікатора відправника повинні використовуватися ім’я емітента сертифіката (**надавача електронних довірчих послуг**) та серійний номер сертифіката відкритого ключа відправника “issuerAndSerialNumber” або ідентифікатор відкритого ключа відправника “subjectKeyIdentifier”; під час застосування динамічного механізму узгодження ключів Діффі-Геллмана як ідентифікаційних даних відправника застосовується його відкритий сеансовий ключ (маркер), що генерується відправником та міститься в полі “originatorKey”; Під час застосування динамічного механізму узгодження ключів у групі точок еліптичної кривої поле “algorithm” поля “originatorKey” для алгоритму цифрового підпису ДСТУ 4145-2002 може мати такі значення: …
4) поле “ukm” (User Keying Material – матеріал щодо ключа користувача) містить додаткову інформацію, яку відправник надає	4) поле “ukm” (User Keying Material – матеріал щодо ключа користувача) містить додаткову інформацію, яку відправник надає

одержувачу під час виконання протоколу узгодження ключа Діффі-Геллмана. Поле "ukm" використовується з метою забезпечення можливості формування різних значень узгоджених ключів у різний час суб'єктами, що використовують ті самі пари ключів (статичні ключі). Реалізації цих Вимог повинні обробляти "KeyAgreeRecipientInfo", що містить поле "ukm". **У разі застосування механізму узгодження ключів у циклічній групі поля в поле "ukm" вноситься значення "partyAInfo" (кодоване як OCTET STRING), яке генерується відправником і використовується в структурі "OtherInfo". Якщо "partyAInfo" задано, то воно повинно мати довжину 512 бітів (64 байти). Параметр "partyAInfo" визначається у позиціях 4 та 6 пункту 6.3 глави 6 розділу V цих Вимог.** У разі застосування динамічного механізму узгодження ключів у групі точок еліптичної кривої (ECDH) у поле "ukm" вноситься значення "entityUInfo" (кодоване як OCTET STRING), яке генерується відправником і використовується в структурі "SharedInfo". Якщо "entityUInfo" задано, то воно повинно мати довжину 512 бітів (64 байти). Параметр "entityUInfo" визначається у позиції 6 пункту 6.4 глави 6 розділу V цих Вимог;	одержувачу під час виконання протоколу узгодження ключа Діффі-Геллмана. Поле "ukm" використовується з метою забезпечення можливості формування різних значень узгоджених ключів у різний час суб'єктами, що використовують ті самі пари ключів (статичні ключі). Реалізації цих Вимог повинні обробляти "KeyAgreeRecipientInfo", що містить поле "ukm". У разі застосування динамічного механізму узгодження ключів у групі точок еліптичної кривої (ECDH) у поле "ukm" вноситься значення "entityUInfo" (кодоване як OCTET STRING), яке генерується відправником і використовується в структурі "SharedInfo". Якщо "entityUInfo" задано, то воно повинно мати довжину 512 бітів (64 байти). Параметр "entityUInfo" визначається у позиції 6 пункту 6.4 глави 6 розділу V цих Вимог;
3.7.5. Особливості синтаксису структури "KeyAgreeRecipientInfo": … **3) об'єктні ідентифікатори (OID) протоколу узгодження ключа у циклічній групі поля:** **протокол узгодження ключа у циклічній групі поля з використанням геш-функції ГОСТ 34.311-95 "Информационная технология. Криптографическая защита информации. Функция хеширования" (далі – ГОСТ 34.311-95) позначається через ідентифікатор "id-DH-ua". Протокол узгодження ключа у циклічній групі поля з використанням геш-функції ГОСТ 34.311-95 є обов'язковим алгоритмом, який застосовується як для статичного, так і для динамічного механізму узгодження ключа; при цьому ознакою динамічного механізму є ненульове значення поля "originatorKey" (відповідно до абзацу третього позиції 3**	3.7.5. Особливості синтаксису структури "KeyAgreeRecipientInfo": …

підпункту 3.7.4 пункту 3.7 глави 3 розділу IV цих Вимог): **id-DH-ua OBJECT IDENTIFIER ::= { iso(1) member-body(2) Ukraine(804) root(2) security(1) cryptography(1) ua-pki (1) alg (1) asym (3) DH-ua(3) };** **для протоколів узгодження ключа у циклічній групі поля з використанням геш-функції SHA-1 відповідно до ДСТУ ISO/IEC 10118-3:2005 та RFC 2631 (тільки для сумісності з реалізаціями засобів КЗІ, що були розроблені до прийняття цих Вимог) використовуються такі ідентифікатори:** **"id-SSDH" – необов'язковий, застосовується для статичного механізму узгодження ключа;** **"id-ESDH" – необов'язковий, застосовується для динамічного механізму узгодження ключа;** **id-SSDH OBJECT IDENTIFIER ::= { iso(1) member-body(2) us(840) rsadsi(113549) pkcs(1) pkcs9(9) smime(16) alg(3) 10 };** **id-ESDH OBJECT IDENTIFIER ::= { iso(1) member-body(2) us(840) rsadsi(113549) pkcs(1) pkcs9(9) smime(16) alg(3) 5 };** **протоколи узгодження ключа, а саме: ZZ-функція та KDF-функція, у циклічній групі поля визначені у розділі V цих Вимог;** **4)** об'єктні ідентифікатори (OID) протоколу узгодження ключа в групі точок еліптичної кривої (ECDH): … протоколи узгодження ключа, визначені ідентифікаторами згідно з **позицією 4** підпункту 3.7.5 пункту 3.7 глави 3 розділу IV цих Вимог, застосовуються як для статичного, так і для динамічного механізму узгодження ключа. При цьому ознакою динамічного механізму є не нульове значення поля "originatorKey" відповідно до абзацу третього позиції 3 підпункту 3.7.4 пункту 3.7 глави 3 розділу IV цих Вимог; протоколи узгодження ключа, а саме ZZ-функція та KDF-функція, у групі точок еліптичної кривої визначено у розділі V цих Вимог.	**3)** об'єктні ідентифікатори (OID) протоколу узгодження ключа в групі точок еліптичної кривої (ECDH): … протоколи узгодження ключа, визначені ідентифікаторами згідно з **позицією 3** підпункту 3.7.5 пункту 3.7 глави 3 розділу IV цих Вимог, застосовуються як для статичного, так і для динамічного механізму узгодження ключа. При цьому ознакою динамічного механізму є не нульове значення поля "originatorKey" відповідно до абзацу третього позиції 3 підпункту 3.7.4 пункту 3.7 глави 3 розділу IV цих Вимог; протоколи узгодження ключа, а саме ZZ-функція та KDF-функція, у групі точок еліптичної кривої визначено у розділі V цих Вимог.

V. Протокол узгодження ключа Діффі-Геллмана	
1. Призначення та порядок використання протоколу узгодження ключа Протокол узгодження ключа призначений для установлення розділеної таємниці (обчислення узгоджувального ключа КШК) на основі використання особистого ключа відправника та відкритого ключа одержувача і навпаки. **У цих Вимогах визначено дві групи протоколів узгодження ключа Діффі-Геллмана: DH – у циклічній групі поля та ECDH – у групі точок еліптичної кривої.**	1. Призначення та порядок використання протоколу узгодження ключа Протокол узгодження ключа призначений для установлення розділеної таємниці (обчислення узгоджувального ключа КШК) на основі використання особистого ключа відправника та відкритого ключа одержувача і навпаки. **У цих Вимогах визначено протокол узгодження ключа Діффі-Геллмана у групі точок еліптичної кривої (ECDH).**
2. Протокол узгодження ключа Діффі-Геллмана, який виконує відправник: отримати параметри відкритого ключа одержувача (із сертифіката відкритого ключа); порівняти параметри відкритого ключа відправника з параметрами відкритого ключа одержувача у разі наявності сертифіката відкритого ключа відправника; установити статичний механізм узгодження ключа у разі еквівалентності параметрів, в іншому випадку встановити динамічний механізм узгодження ключа та виконати обчислення ключової пари, використовуючи алгоритм та відповідні параметри ключа одержувача; виконати обчислення спільного секрету (ZZ) **для визначеного протоколу в циклічній групі поля або в групі точок еліптичної кривої**; виконати обчислення ключа шифрування ключа КШК (KDF – Key Derivation Function).	2. Протокол узгодження ключа Діффі-Геллмана, який виконує відправник: отримати параметри відкритого ключа одержувача (із сертифіката відкритого ключа); порівняти параметри відкритого ключа відправника з параметрами відкритого ключа одержувача у разі наявності сертифіката відкритого ключа відправника; установити статичний механізм узгодження ключа у разі еквівалентності параметрів, в іншому випадку встановити динамічний механізм узгодження ключа та виконати обчислення ключової пари, використовуючи алгоритм та відповідні параметри ключа одержувача; виконати обчислення спільного секрету (ZZ); виконати обчислення ключа шифрування ключа КШК (KDF – Key Derivation Function).
3. Протокол узгодження ключа Діффі-Геллмана, що виконується одержувачем: завантажити сертифікат і особистий ключ одержувача та отримати параметри ключової пари відправника; отримати ASN.1 “EnvelopedData”; на основі аналізу “EnvelopedData” визначити механізм узгодження ключа. Ознакою динамічного механізму є ненульове значення поля “originatorKey” відповідно до позиції 3 підпункту 3.7.4 пункту 3.7 глави 3 розділу IV цих Вимог;	3. Протокол узгодження ключа Діффі-Геллмана, що виконується одержувачем: завантажити сертифікат і особистий ключ одержувача та отримати параметри ключової пари відправника; отримати ASN.1 “EnvelopedData”; на основі аналізу “EnvelopedData” визначити механізм узгодження ключа. Ознакою динамічного механізму є ненульове значення поля “originatorKey” відповідно до позиції 3 підпункту 3.7.4 пункту 3.7 глави 3 розділу IV цих Вимог;

якщо механізм статичний, отримати сертифікат відправника. Сертифікат відправника може міститися у структурі “OriginatorInfo”, в іншому випадку він має бути отриманий одержувачем із його сховища сертифікатів за даними з поля “OriginatorIdentifierOrKey”; отримати із сертифіката відправника відкритий ключ; отримати параметри відкритого ключа відправника; порівняти параметри ключа пари одержувача з параметрами відкритого ключа відправника; нееквівалентність параметрів означає помилку. Необхідно припинити оброблення; у разі еквівалентності параметрів перейти до наступного кроку цього протоколу; якщо механізм динамічний, отримати динамічний відкритий ключ відправника зі структури “EnvelopedData”; виконати обчислення спільного секрету (ZZ) **для визначеного протоколу в циклічній групі поля або в групі точок еліптичної кривої**; виконати обчислення ключа шифрування ключа КШК (KDF – Key Derivation Function).	якщо механізм статичний, отримати сертифікат відправника. Сертифікат відправника може міститися у структурі “OriginatorInfo”, в іншому випадку він має бути отриманий одержувачем із його сховища сертифікатів за даними з поля “OriginatorIdentifierOrKey”; отримати із сертифіката відправника відкритий ключ; отримати параметри відкритого ключа відправника; порівняти параметри ключа пари одержувача з параметрами відкритого ключа відправника; нееквівалентність параметрів означає помилку. Необхідно припинити оброблення; у разі еквівалентності параметрів перейти до наступного кроку цього протоколу; якщо механізм динамічний, отримати динамічний відкритий ключ відправника зі структури “EnvelopedData”; виконати обчислення спільного секрету (ZZ); виконати обчислення ключа шифрування ключа КШК (KDF – Key Derivation Function).

4.1. Параметри протоколу узгодження ключа у циклічній групі поля:
 	
1) загальносистемні параметри протоколу id-ESDH-ua можуть визначатися як ASN.1 структура:
DHParameters ::= SEQUENCE {
p INTEGER,
q INTEGER,
a INTEGER,
validationParms GOST34310ValidationParms OPTIONAL,
-- параметри валідації,
dke OCTET STRING OPTIONAL }
GOST34310ValidationParms ::= SEQUENCE {
x0 INTEGER,
c INTEGER,
	-

<table>
<tr>
<td>
d INTEGER OPTIONAL };
2) значення полів структури “DHParameters” наведено в таблиці.
Таблиця
<table>
<tr><td>p</td><td>характеристика основного поля, просте число (modulus)</td></tr>
<tr><td>q</td><td>порядок циклічної підгрупи (order of cyclic group)</td></tr>
<tr><td>a</td><td>твірний елемент циклічної підгрупи (generator)</td></tr>
<tr><td>dke</td><td>довгостроковий ключовий елемент (ДКЕ)</td></tr>
<tr><td>x0</td><td>початковий стан, що використовувався для генерації p, q</td></tr>
<tr><td>c</td><td>параметр датчика, що використовувався для генерації p,</td></tr>
<tr><td>d</td><td>довільне число, що використовувалося для генерації a, 1</td></tr>
</table>
3) операція порівняння загальносистемних параметрів “DHParameters”.
При визначенні механізму узгодження ключів повинна виконуватися операція порівняння загальносистемних параметрів. Якщо загальносистемні параметри – еквівалентні, то застосовується статичний механізм узгодження ключів, в інших випадках – динамічний.
При виконанні операції порівняння параметрів повинні порівнюватися параметри p, a, q та додатково dke (у разі використання протоколу “id-ESDHua”).
Параметри валідації “GOST34310ValidationParms” як необов’язкові не повинні використовуватися в операції порівняння.
</td>
<td></td>
</tr>
<tr>
<td>
4.2. Параметри протоколу узгодження ключа в групі точок еліптичної кривої:
…
</td>
<td>
4.1. Параметри протоколу узгодження ключа в групі точок еліптичної кривої:
…
</td>
</tr>
<tr>
<td>
4.3. Кодування ДКЕ виконується як:
dke OCTET STRING.
ДКЕ може кодуватися в розгорнутому або упакованому форматі залежно від алгоритму:
для ДСТУ 4145-2002 - упакований формат;
для ГОСТ 34.310-95 - розгорнутий формат.
За відсутності ДКЕ в параметрах криптоалгоритму використовується ДКЕ № 1 Переліку ДКЕ, які рекомендуються до застосування у засобах КЗІ, наведеному у додатку 1 до Інструкції № 114.
</td>
<td>
4.2. Кодування ДКЕ виконується як:
dke OCTET STRING.
Для ДСТУ 4145-2002 ДКЕ кодується в упакованому форматі.
За відсутності ДКЕ в параметрах криптоалгоритму використовується ДКЕ № 1 Переліку ДКЕ, які рекомендуються до застосування у засобах КЗІ, наведеному у додатку 1 до Інструкції № 114.
Спосіб представлення ДКЕ № 1 повинен відповідати вимогам до
</td>
</tr>
</table>

Спосіб представлення ДКЕ № 1 повинен відповідати вимогам **пункту 3.12 розділу III Вимог до формату посиленого сертифіката відкритого ключа.**	технічних засобів, процесів їх створення, використання та функціонування у складі інформаційно-телекомунікаційних систем під час надання кваліфікованих електронних довірчих послуг, **встановлених у нормативно-правових актах Мін'юсту та Адміністрації Держспецзв'язку.**
5.1. Обчислення спільного секрету у циклічній групі поля (DH) ґрунтується на RFC 2631 та ДСТУ ISO/IEC 11770-3:2015 і виконується таким чином: **Z = (yb ^ xa) mod p = (ya ^ xb) mod p,** **де Z – спільний секрет як елемент поля, в якому виконується обчислення;** **"^" – означає операцію піднесення до ступеня;** **"xa" – особистий ключ відправника;** **"ya" – відкритий ключ відправника;** **"xb" – особистий ключ одержувача;** **"yb" – відкритий ключ одержувача;** **"p" – характеристика поля, непарне просте число (odd prime);** **"a" – твірний елемент циклічної підгрупи, генератор (generator).** **Відправником виконується обчислення за формулою** **Z = (yb ^ xa) mod p.** **Одержувачем виконується обчислення за формулою** **Z = (ya ^ xb) mod p.** **Алгоритм DH не повинен застосовуватися, якщо:** **a^x = a (mod p) або a^y = a (mod p),** **де x – особистий ключ;** **y – відкритий ключ.**	-
5.2. Обчислення спільного секрету в групі точок еліптичної кривої (ECDH). …	**5.1**. Обчислення спільного секрету в групі точок еліптичної кривої (ECDH). …
5.3. Перетворення елемента поля Z на рядок байтів ZZ. Для використання у функціях формування ключа (KDF-функціях) спільного секрету Z, отриманого згідно з **пунктом 5.1 глави**	**5.2.** Перетворення елемента поля Z на рядок байтів ZZ. Для використання у функціях формування ключа (KDF-функціях) спільного секрету Z, отриманого згідно з абзацом четвертим пункту **5.1**

5 розділу V та **абзацом четвертим пункту 5.2 глави 5 розділу V** цих Вимог, необхідно перетворити елемент поля Z на рядок байтів ZZ (Field-Element-to-Octet-String Conversion). Таке перетворення повинно виконуватися так. … Приклади перетворення елемента поля на рядок байтів у форматі Big-Endian, обчислення спільного секрету ZZ **у циклічній групі простого поля та у групі точок еліптичної кривої** розміщуються на офіційному веб-сайті Державної служби спеціального зв'язку та захисту інформації України.	глави 5 розділу V цих Вимог, необхідно перетворити елемент поля Z на рядок байтів ZZ (Field-Element-to-Octet-String Conversion). Таке перетворення повинно виконуватися так. … Приклади перетворення елемента поля на рядок байтів у форматі Big-Endian, обчислення спільного секрету ZZ розміщуються на офіційному веб-сайті Державної служби спеціального зв'язку та захисту інформації України.
6.3. KDF-функція у циклічній групі поля: 1) функція формування ключа (KDF-функція) у циклічній групі поля (DHKDF) ґрунтується на RFC 2631 та ДСТУ ISO/IEC 11770-3:2015; … 7) приклади обчислення ключа КШК у циклічній групі поля розміщуються на офіційному веб-сайті Державної служби спеціального зв'язку та захисту інформації України.	-
6.4. Використання KDF-функції в групі точок еліптичної кривої (ECDH): **1) функція формування ключа (KDF-функція) у циклічній групі поля ґрунтується на ДСТУ ISO/IEC 15946-3:2002;** 2) формування ключового матеріалу KM: KM = H (ZZ || counter || SharedInfo), де KM – ключовий матеріал (рядок байтів), довжина якого залежить від алгоритму H; H – геш-функція, яка визначається ідентифікаторами протоколу узгодження, що визначені у **позиції 4** підпункту 3.7.5 пункту 3.7 глави 3 розділу IV цих Вимог; ZZ – спільний секрет, обчислений відповідно до пункту 5.3 глави 5 розділу V цих Вимог; … 4) поля структури "SharedInfo": "algorithm" – ідентифікатор алгоритму ключа шифрування ключа (KeyWrapAlgorithm), на якому повинен бути зашифрований	**6.3.** Використання KDF-функції в групі точок еліптичної кривої (ECDH): **1) KDF-функція в групі точок еліптичної кривої (ECDH) ґрунтується на ДСТУ ISO/IEC 11770-3:2015.** 2) формування ключового матеріалу KM: KM = H (ZZ || counter || SharedInfo), де KM – ключовий матеріал (рядок байтів), довжина якого залежить від алгоритму H; H – геш-функція, яка визначається ідентифікаторами протоколу узгодження, що визначені у **позиції 3** підпункту 3.7.5 пункту 3.7 глави 3 розділу IV цих Вимог; ZZ – спільний секрет, обчислений відповідно до пункту 5.3 глави 5 розділу V цих Вимог; … 4) поля структури "SharedInfo": "algorithm" – ідентифікатор алгоритму ключа шифрування ключа (KeyWrapAlgorithm), на якому повинен бути зашифрований ключ

ключ шифрування повідомлення (даних). Параметри алгоритму повинні бути NULL (ASN.1 NULL); "entityUInfo" – випадковий рядок **(аналогічний полю "partyAInfo" структури "OtherInfo", наведеної у позиції 3 пункту 6.3 глави 6 розділу V цих Вимог)**, який генерує відправник. У CMS це значення розміщується в полі "ukm" ("UserKeyingMaterial") (закодоване як OCTET STRING) структури "KeyAgreeRecipientInfo". Довжина "entityUInfo" повинна бути 512 бітів (64 байти); "suppPubInfo" – довжина сформованого ключа КШК у бітах **(аналогічно полю "suppPubInfo" структури "OtherInfo", наведеної у позиції 3 пункту 4.1 глави 4 розділу V)**, представлена як бітовий вектор (чотири байти) 32-бітного числа. Наприклад, ключ 192 біти повинен бути представлений як бітовий вектор "00 00 00 C0" (hex);	шифрування повідомлення (даних). Параметри алгоритму повинні бути NULL (ASN.1 NULL); "entityUInfo" – випадковий рядок, який генерує відправник. У CMS це значення розміщується в полі "ukm" ("UserKeyingMaterial") (закодоване як OCTET STRING) структури "KeyAgreeRecipientInfo". Довжина "entityUInfo" повинна бути 512 бітів (64 байти); "suppPubInfo" – довжина сформованого ключа КШК у бітах, представлена як бітовий вектор (чотири байти) 32-бітного числа. Наприклад, ключ 192 біти повинен бути представлений як бітовий вектор "00 00 00 C0" (hex);
VI. Алгоритм захисту ключа шифрування даних "KeyWrapAlgorithm"	
4. Ключ узгодження КШК формується за **алгоритмами узгодження ключа DH або** ECDH: KeyWrapAlgorithm ::= AlgorithmIdentifier.	4. Ключ узгодження КШК формується за **алгоритмом** ECDH: KeyWrapAlgorithm ::= AlgorithmIdentifier.
VIII. Сертифікат шифрування	
8.1 Сертифікат шифрування у цих Вимогах призначається для використання у протоколах узгодження ключа Діффі-Геллмана: **DH в циклічній групі простого поля та** в групі точок еліптичної кривої.	8.1 Сертифікат шифрування у цих Вимогах призначається для використання **у протоколі узгодження ключа Діффі-Геллмана в групі точок еліптичної кривої.**
8.2 Формат сертифіката шифрування повинен відповідати **Вимогам до формату посиленого сертифіката відкритого ключа.**	8.2 Формат сертифіката шифрування повинен відповідати **формату кваліфікованого сертифіката відкритого ключа, встановленого у Вимогах до електронних довірчих послуг**
8.3 Розширення сертифіката шифрування "Використання ключа". Розширення "Використання ключа" має такий об'єктний ідентифікатор: id-ce-keyUsage OBJECT IDENTIFIER::= {id-ce 15}. У розширенні "Використання ключа" ("keyUsage") повинно бути встановлено значення "узгодження ключа" ("keyAgreement"). Додатково можуть бути встановлені значення: "тільки зашифрування" ("encipherOnly"); "тільки розшифрування" ("decipherOnly"). У розширенні "Використання ключа" ("keyUsage") не повинні	8.3 Розширення сертифіката шифрування "Використання ключа". Розширення "Використання ключа" має такий об'єктний ідентифікатор: id-ce-keyUsage OBJECT IDENTIFIER::= {id-ce 15}. У розширенні "Використання ключа" ("keyUsage") повинно бути встановлено значення "узгодження ключа" ("keyAgreement"). Додатково можуть бути встановлені значення: "тільки зашифрування" ("encipherOnly"); "тільки розшифрування" ("decipherOnly"). У розширенні "Використання ключа" ("keyUsage") не повинні бути встановлені значення:

бути встановлені значення: “**електронний** цифровий підпис” (“digitalSignature”); “**електронний** цифровий підпис у сертифікаті” (“keyCertSign ”); “**електронний** цифровий підпис у списку відкликаних сертифікатів” (“crlSign”); “неспростовність” (“nonRepudiation”); “шифрування ключа” (“keyEncipherment”); “підписування сертифікатів” (“keyCertSign”); “підписування списків відкликаних сертифікатів” (“cRLSign”).	“цифровий підпис” (“digitalSignature”); “цифровий підпис у сертифікаті” (“keyCertSign ”); “цифровий підпис у списку відкликаних сертифікатів” (“crlSign”); “неспростовність” (“nonRepudiation”); “шифрування ключа” (“keyEncipherment”); “підписування сертифікатів” (“keyCertSign”); “підписування списків відкликаних сертифікатів” (“cRLSign”).
Наказ Адміністрації Держспецзв’язку від 12 червня 2007 року № 114 «Про затвердження Інструкції про порядок постачання і використання ключів до засобів криптографічного захисту інформації», зареєстрований в Міністерстві юстиції України 25 червня 2007 року за № 729/13996 (зі змінами)	
Інструкція про порядок постачання і використання ключів до засобів криптографічного захисту інформації	
За текстсом слова та цифри **«ГОСТ 28147-89»** замінити словами та цифрами **«ДСТУ ГОСТ 28147:2009»**	
1. Загальні положення	
1.1. Інструкція про порядок постачання і використання ключів до засобів криптографічного захисту інформації (далі – Інструкція) розроблена відповідно до Законів України „Про інформацію”, „Про Державну службу спеціального зв’язку та захисту інформації України”, „Про **електронний цифровий підпис”,** „Про захист інформації в інформаційно-телекомунікаційних системах”, Положення про Адміністрацію Державної служби спеціального зв’язку та захисту інформації, затвердженого постановою Кабінету Міністрів України від 24.06.2006 № 868.	1.1. Інструкція про порядок постачання і використання ключів до засобів криптографічного захисту інформації (далі – Інструкція) розроблена відповідно до Законів України „Про інформацію”, „Про Державну службу спеціального зв’язку та захисту інформації України”, „Про **електронні довірчі послуги”,** „Про захист інформації в інформаційно-телекомунікаційних системах”, Положення про Адміністрацію Державної служби спеціального зв’язку та захисту інформації, затвердженого постановою Кабінету Міністрів України від 24.06.2006 № 868.
1.2. Інструкція встановлює порядок постачання та використання ключів до засобів криптографічного захисту інформації (далі – КЗІ), які реалізують криптографічний алгоритм, визначений **ГОСТ 28147-89** „Системы обработки информации. Защита криптографическая. Алгоритм криптографического преобразования” (далі - ГОСТ 28147-89).	1.2. Інструкція встановлює порядок постачання та використання ключів до засобів криптографічного захисту інформації (далі – КЗІ), які реалізують криптографічний алгоритм, визначений **ДСТУ ГОСТ 28147:2009** «Системы обработки информации. Защита криптографическая. Алгоритм криптографического преобразования» (далі - **ДСТУ** ГОСТ 28147-89).

1.3. Вимоги цієї Інструкції обов`язкові для виконання органами державної влади та органами місцевого самоврядування, підприємствами, установами та організаціями всіх форм власності, які здійснюють розроблення, виробництво, використання, експлуатацію, сертифікаційні випробування, тематичні дослідження, експертизу, увезення, вивезення криптосистем і засобів КЗІ, що реалізують криптографічний алгоритм, визначений **ГОСТ 28147-89**, надають послуги в галузі КЗІ з використанням зазначених засобів КЗІ (у тому числі **послуги електронного цифрового підпису**), здійснюють їх постачання або торгівлю ними.	1.3. Вимоги цієї Інструкції обов`язкові для виконання органами державної влади та органами місцевого самоврядування, підприємствами, установами та організаціями всіх форм власності, які здійснюють розроблення, виробництво, використання, експлуатацію, сертифікаційні випробування, тематичні дослідження, експертизу, увезення, вивезення криптосистем і засобів КЗІ, що реалізують криптографічний алгоритм, визначений **ДСТУ ГОСТ 28147:2009**, надають послуги в галузі КЗІ з використанням зазначених засобів КЗІ (у тому числі **електронні довірчі послуги**), здійснюють їх постачання або торгівлю ними.
1.5. Використані в цій Інструкції терміни мають такі значення: довгостроковий ключовий елемент (далі – ДКЕ) – ключ, що визначає заповнення таблиць блока підстановки алгоритму криптографічного перетворення, визначеного **ГОСТ 28147-89**; замовник – юридична особа будь-якої форми власності, яка замовляє встановленим порядком ключі до засобів КЗІ, у тому числі **засобів електронного цифрового підпису**, у яких реалізується криптографічний алгоритм, визначений **ГОСТ 28147-89**. Як замовники можуть виступати розробники, виробники, постачальники та користувачі засобами КЗІ; методика генерації ключів – опис послідовності операцій (алгоритму), що виконуються у процесі генерації ключів; методика розподілу ключів – опис послідовності операцій (алгоритму), що виконуються у мережі захищеного інформаційного обміну з метою формування (отримання) необхідних ключів; носій ключової інформації (далі – НКІ) – матеріальний носій інформації, що призначений для запису та збереження ключів; постачальник – підприємство, установа, організація або підрозділ Державної служби спеціального зв'язку та захисту інформації України (далі – Держспецзв`язку), які визначаються	1.5. Використані в цій Інструкції терміни мають такі значення: довгостроковий ключовий елемент (далі – ДКЕ) – ключ, що визначає заповнення таблиць блока підстановки алгоритму криптографічного перетворення, визначеного **ДСТУ ГОСТ 28147:2009**; замовник – юридична особа будь-якої форми власності, яка замовляє встановленим порядком ключі до засобів КЗІ, у тому числі **засобів удосконаленого електронного підпису чи печатки, засобів кваліфікованого електронного підпису чи печатки**, у яких реалізується криптографічний алгоритм, визначений **ДСТУ ГОСТ 28147:2009**. Як замовники можуть виступати розробники, виробники, постачальники та користувачі засобами КЗІ; методика генерації ключів – опис послідовності операцій (алгоритму), що виконуються у процесі генерації ключів; методика розподілу ключів – опис послідовності операцій (алгоритму), що виконуються у мережі захищеного інформаційного обміну з метою формування (отримання) необхідних ключів; носій ключової інформації (далі – НКІ) – матеріальний носій інформації, що призначений для запису та збереження ключів; постачальник – підприємство, установа, організація або підрозділ Державної служби спеціального зв'язку та захисту інформації України (далі – Держспецзв`язку), які визначаються Держспецзв`язку для

Держспецзв`язку для здійснення постачання ключових документів до засобів КЗІ; разовий (сеансовий) ключ (далі – РК) – ключ, який визначає порядок заповнення ключового запам'ятовувального пристрою засобу КЗІ, що реалізує алгоритм криптографічного перетворення, визначений **ГОСТ 28147-89**. Інші терміни застосовуються у значеннях, наведених у нормативно-правових актах з питань криптографічного захисту інформації, **електронного цифрового підпису**, а також **ГОСТ 28147-89**.	здійснення постачання ключових документів до засобів КЗІ; разовий (сеансовий) ключ (далі – РК) – ключ, який визначає порядок заповнення ключового запам'ятовувального пристрою засобу КЗІ, що реалізує алгоритм криптографічного перетворення, визначений **ДСТУ ГОСТ 28147:2009**. Інші терміни застосовуються у значеннях, наведених у нормативно-правових актах з питань криптографічного захисту інформації, **електронних довірчих послуг**, а також **ДСТУ ГОСТ 28147:2009**.
2. Порядок використання ключів	
2.4. У випадках, передбачених пунктом 2.3 цієї Інструкції, ДКЕ можуть також обиратися з **посилених** сертифікатів відкритого ключа **електронного цифрового підпису**.	2.4. У випадках, передбачених пунктом 2.3 цієї Інструкції, ДКЕ можуть також обиратися з сертифікатів відкритого ключа.

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

04/02/03-2709
19.09.19

Прим. № 4

ПОЯСНЮВАЛЬНА ЗАПИСКА

до проєкту наказу Адміністрації Державної служби спеціального зв'язку та захисту інформації України «Про затвердження Змін до деяких наказів Адміністрації Державної служби спеціального зв'язку та захисту інформації України»

Мета: приведення нормативно-правових актів Адміністрації Державної служби спеціального зв'язку та захисту інформації України у відповідність до вимог законодавства у сфері електронних довірчих послуг та уточнення застосування їх вимог.

1. Підстава розроблення проєкту акта

Проєкт наказу Адміністрації Державної служби спеціального зв'язку та захисту інформації України «Про затвердження Змін до деяких наказів Адміністрації Державної служби спеціального зв'язку та захисту інформації України» (далі – проєкт наказу) розроблено на виконання:

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

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 1910 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

У зв'язку із зміною законодавства у сферах електронного цифрового підпису, втрати та набрання чинності низки стандартів з питань методів захисту, інформаційної безпеки, технічної документації на продукцію, та з метою уточнення застосування деяких вимог потребують змін такі нормативно-правові акти Адміністрації Держспецзв'язку у сфері криптографічного захисту інформації (далі – КЗІ):

Положення про порядок розроблення, виробництва та експлуатації засобів криптографічного захисту інформації, затверджене наказом Адміністрації Держспецзв'язку від 20 липня 2007 року № 141 (далі – Положення № 141);

Положення про державну експертизу в сфері криптографічного захисту інформації, затверджене наказом Адміністрації Держспецзв'язку від 23 червня 2008 року № 100 (далі - Положення № 100);

наказ Адміністрації Держспецзв'язку від 18 грудня 2012 року № 739 «Про затвердження вимог до форматів криптографічних повідомлень» (далі - Наказ № 739);

Вимоги до форматів криптографічних повідомлень, затвердженні Наказом № 739 (далі - Вимоги № 739);

Інструкція про порядок постачання і використання ключів до засобів криптографічного захисту інформації, затверджена наказом Адміністрації Держспецзв'язку від 12 червня 2007 року № 114 (далі - Інструкція № 114).

3. Суть проєкту акта

Проєктом наказу пропонується внести такі зміни до наказів Адміністрації Держспецзв'язку:

1) до Положення № 141, що стосуються: поширення сфери застосування акту на засоби УЕП та КЕП (замість засобів ЕЦП); уточнення термінології; взаємоузгодження пунктів 1 та 5 розділу I; запровадження умов експлуатації засобів КЗІ за наявності документа про відповідність або позитивного експертного висновку за результатами державної експертизи у сфері КЗІ, що підтверджує клас засобу КЗІ (рівень гарантій) та реалізовані для цього методи захисту (згідно з розділом II Положення № 141); встановлення особливостей розроблення, експлуатації та обліку засобів УЕП та КЕП з посиланням на відповідні нормативно-правові акти у сфері електронних довірчих послуг;

2) до Положення № 100, що стосуються: уточнення термінології, у тому числі заміни об'єкту експертизи «програмно-технічний комплекс ЦСК» на - «криптосистеми, що використовується для надання кваліфікованих електронних довірчих послуг, або в схемах електронної ідентифікації»; встановлення обов'язковості проходження державної експертизи у сфері КЗІ для засобів КЗІ, що використовуються для забезпечення функціонування державної системи урядового зв'язку; встановлення вимог до оформлення експертного висновку за результатами державної експертизи у сфері КЗІ; виключення посилань на стандарти, що втратили чинність (ДСТУ 1.3:2004, ГОСТ 2.114-95, ГОСТ 19.201-78, ГОСТ 19.202-78, ГОСТ 19.401-78, ГОСТ 19.402-78, ГОСТ 19.301-79, ГОСТ 19.503.79, ГОСТ 19.504-79, ГОСТ 19.505-79).

3) до Наказу № 739, що стосуються: звуження сфери його застосування до обсягу необхідного для забезпечення сумісності державних електронних сервісів, орієнтованих на використання кваліфікованих електронних довірчих послуг, із встановленими Вимогами № 739 форматами даних;

4) до Вимог № 739, що стосуються: уточнення термінології, виключення протоколу узгодження ключів у циклічній групі поля (оскільки стандарт ГОСТ 34.310-95 вже не застосовується в інфраструктурі відкритих ключів України);

5) до Наказу № 114, що стосуються уточнення термінології.

4. Правові аспекти

Правовими підставами розроблення проєкту наказу є:

Закон України «Про електронні довірчі послуги»;

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

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

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

У зв'язку зі зміною сфери державного регулювання електронного цифрового підпису на електронні довірчі послуги потребують скасування нормативно-правові акти:

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

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

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

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

Проєкт 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

Реалізація проєкту наказу не потребує додаткових матеріальних та інших витрат.

6. Прогноз впливу

Реалізація проекту наказу справлятиме вплив на ринкове середовище, забезпечення прав та інтересів суб'єктів господарювання, що надають 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.

6^1. Стратегічна екологічна оцінка

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

7. Позиція заінтересованих сторін

Проєкт наказу підлягає проведенню консультацій з суб'єктами господарювання, що надають кваліфіковані електронні довірчі послуги.

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

За предметом правового регулювання 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.

8. Громадське обговорення

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

9. Позиція заінтересованих органів

Проєкт наказу підлягає погодженню з Міністерством розвитку економіки, торгівлі та сільського господарства України, Міністерством фінансів України, Державним агентством з питань електронного урядування України, Державною регуляторною службою, Антимонопольним комітетом України, Національним

банком України, Міністерством освіти і науки України, Державним комітетом телебачення та радіомовлення України, Національною комісією, що здійснює державне регулювання у сфері зв'язку та інформатизації, Державною службою України з питань безпечності харчових продуктів та захисту споживачів.

10. Правова експертиза

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

11. Запобігання дискримінації

У проєкті наказу відсутні положення, які містять ознаки дискримінації.

Проєкт наказу не потребує проведення громадської антидискримінаційної експертизи.

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

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

12. Запобігання корупції

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

Проєкт наказу не потребує проведення громадської антикорупційної експертизи.

13. Прогноз результатів

Прийняття проєкту наказу дозволить:

врегулювати термінологію відповідно до чинного законодавства;

забезпечити підтвердження класу засобу КЗІ та реалізованих для цього методів захисту;

забезпечити встановлення особливостей розроблення, експлуатації та обліку засобів удосконаленого/кваліфікованого електронного підпису або печатки.

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

«18» вересня 2019 року

09/03/02-2710
19.09.19

ПРОГНОЗ ВПЛИВУ

реалізації проєкту наказу Адміністрації Державної служби спеціального зв'язку та захисту інформації України «Про затвердження Змін до деяких наказів Адміністрації Державної служби спеціального зв'язку та захисту інформації України»

1. Суть проєкту акта

Проєкт наказу Адміністрації Державної служби спеціального зв'язку та захисту інформації України «Про затвердження Змін до деяких наказів Адміністрації Державної служби спеціального зв'язку та захисту інформації України» спрямований на приведення нормативно-правових актів Адміністрації Держспецзв'язку у відповідність до вимог законодавства у сфері електронних довірчих послуг та уточнення застосування їх вимог.

2. Вплив проєкту акта на ключові інтереси заінтересованих сторін

Заінтересована сторона	Ключовий інтерес	Очікуваний (позитивний чи негативний) вплив на ключовий інтерес із зазначенням передбачуваної динаміки змін основних показників (у числовому або якісному вимірі)		Пояснення (чому саме реалізація акта призведе до очікуваного впливу)
		короткостроковий вплив (до року)	середньостроковий вплив (більше року)	
Громадяни (користувачі електронних довірчих послуг)	Можливість використання засобів УЕП, засобів КЕП відповідно до вимог Закону, та сертифікатів шифрування	**Очікуваний позитивний вплив:** підвищення рівня довіри до кваліфікованих електронних довірчих послуг; можливість конфіденційного обміну даними під час отримання електронних послуг від державних органів	**Очікуваний позитивний вплив:** підвищення рівня довіри до кваліфікованих електронних довірчих послуг; можливість конфіденційного обміну даними під час отримання електронних послуг від державних органів	Реалізація акта призведе до забезпечення належного захисту конфіденційної інформації користувачів електронних довірчих послуг внаслідок наявності якісної продукції, послуг та сервісів
Суб'єкти господарювання (кваліфіковані надавачі електронних довірчих послуг)	Можливість використання засобів удосконаленого електронного підпису чи печатки (засоби УЕП), засобів кваліфікованого електронного підпису чи печатки (засоби	**Очікуваний позитивний вплив:** забезпечення використання під час надання кваліфікованих електронних довірчих послуг засобів УЕП, засобів КЕП, що мають позитивний експертний висновок за	**Очікуваний позитивний вплив:** підвищенню попиту на послуги через підвищення рівня довіри до них, можливістю розширення функціоналу (обслуговування сертифікатів шифрування), сумісного з державними	Реалізація акта призведе до збільшення кількості користувачів електронних довірчих послуг внаслідок покращення якості електронних довірчих послуг.

	КЕП) відповідно до вимог Закону України «Про електронні довірчі послуги» (далі – Закон) та обслуговування сертифікатів шифрування	результатами державної експертизи у сфері КЗІ (вимога Закону України «Про електронні довірчі послуги»)	сервісами та як наслідок: збільшення кількості користувачів електронних довірчих послуг збільшення прибутку кваліфікованих надавачів електронних довірчих послуг	
Держава	Взаємоузгодження вимог законодавства, дотримання принципів державної регуляторної політики	**Очікуваний позитивний вплив:** створення умов для розроблення та оцінки відповідності засобів УЕП, засобів КЕП відповідно до вимог Закону	**Очікуваний позитивний вплив:** створення умов для розроблення та оцінки відповідності засобів УЕП, засобів КЕП відповідно до вимог Закону	Створення умов для розроблення та оцінки відповідності засобів УЕП, засобів КЕП відповідно до вимог Закону досягається шляхом приведення нормативно-правових актів Адміністрації Держспецзв'язку у відповідність до вимог законодавства у сфері електронних довірчих послуг та уточнення застосування їх вимог

АНАЛІЗ РЕГУЛЯТОРНОГО ВПЛИВУ

проєкту наказу Адміністрації Державної служби спеціального зв'язку та захисту інформації України «Про затвердження Змін до деяких наказів Адміністрації Державної служби спеціального зв'язку та захисту інформації України»

І. Визначення проблеми

У зв'язку із зміною законодавства у сферах електронного цифрового підпису, втрати та набрання чинності низки стандартів з питань методів захисту, інформаційної безпеки, технічної документації на продукцію, та з метою уточнення застосування деяких вимог потребують змін такі нормативно-правові акти Адміністрації Держспецзв'язку у сфері криптографічного захисту інформації (далі – КЗІ):

Положення про порядок розроблення, виробництва та експлуатації засобів криптографічного захисту інформації, затверджене наказом Адміністрації Держспецзв'язку від 20 липня 2007 року № 141 (далі – Положення № 141);

Положення про державну експертизу в сфері криптографічного захисту інформації, затверджене наказом Адміністрації Держспецзв'язку від 23 червня 2008 року № 100 (далі - Положення № 100);

наказ Адміністрації Держспецзв'язку від 18 грудня 2012 року № 739 «Про затвердження вимог до форматів криптографічних повідомлень» (далі - Наказ № 739);

Вимоги до форматів криптографічних повідомлень, затвердженні Наказом № 739 (далі - Вимоги № 739);

Інструкція про порядок постачання і використання ключів до засобів криптографічного захисту інформації, затверджена наказом Адміністрації Держспецзв'язку від 12 червня 2007 року № 114 (далі - Інструкція № 114).

До основних проблем, що потребують вирішення віднесено наступні.

1. Неузгодженість положень нормативно-правових актів у сфері криптографічного захисту інформації із законодавством у сфері електронних довірчих послуг.

Так, 05 жовтня 2017 року Верховною Радою України прийнято Закон України «Про електронні довірчі послуги», який набрав чинності 07 листопада 2018 року.

У зв'язку з набранням чинності Законом України «Про електронні довірчі послуги» (далі – Закон) втратив чинність Закон України «Про електронний цифровий підпис».

Пунктом 8 розділу VII «Прикінцеві та перехідні положення» Закону передбачено Кабінету Міністрів України протягом року з дня набрання чинності Законом: привести свої нормативно-правові акти у відповідність із Законом; прийняти нормативно-правові акти, передбачені Законом; забезпечити приведення нормативно-правових актів міністерств та інших центральних органів виконавчої влади у відповідність із Законом.

Таким чином нормативно-правові акти Адміністрації Держспецзв'язку потребують приведення у відповідність із Законом, зокрема в частині поширення сфери їх дії на засоби удосконаленого електронного підпису чи печатки (далі – засоби УЕП) та засоби кваліфікованого електронного підпису чи печатки (далі – засоби КЕП) замість засобів електронного цифрового підпису (далі – засоби ЕЦП), взаємоузгодження їх з актами Кабінету Міністрів України прийнятих на виконання Закону, а також застосування термінології відповідно до Закону.

2. Чинним законодавством у сфері КЗІ не врегульовано питання доведення до споживача інформації про засіб КЗІ у обсязі, необхідному для коректного його застосування.

Так, відповідно до пункту 9 Положення про порядок розроблення, виробництва та експлуатації засобів криптографічного захисту інформації, затвердженим Наказом № 141, з урахуванням установленого рівня можливостей порушника обирається необхідний клас засобів КЗІ (відповідність засобу КЗІ встановленим вимогам).

Водночас інформація про клас засобу КЗІ та реалізовані методи захисту, що забезпечують відповідність такому класу, у позитивному експертному висновку за результатами державної експертизи у сфері КЗІ не вказується.

3. Чинним законодавством у сфері КЗІ не врегульовано питання обов'язковості проведення державної експертизи у сфері КЗІ продукції, чутливої для забезпечення функціонування, безпеки та розвитку державної системи урядового зв'язку.

Так, відповідно до пункту 13 частини першої статті 14 Закону України «Про Державну службу спеціального зв'язку та захисту інформації України» на Держспецзв'язку покладено обов'язок забезпечення функціонування, безпеки та розвитку державної системи урядового зв'язку, її готовності до роботи в особливий період і в разі виникнення надзвичайної ситуації. З метою виконання покладених на Держспецзв'язку обов'язків потребують проведення обов'язкової державної експертизи у сфері КЗІ такі засоби:

засоби, що реалізують криптоперетворення та/або механізми імітозахисту, та використовуються в системах зв'язку, управління та озброєння;

засоби обробки та передачі державних інформаційних ресурсів або інформації, вимога щодо захисту якої встановлена законом, які реалізують функції КЗІ.

4. Чинним законодавством у сфері КЗІ не враховано актуальний стан нормативної бази у сфері інформаційної безпеки та захисту інформації.

Так, у зв'язку із втратою та/або набранням чинності низки стандартів з питань методів захисту, інформаційної безпеки, технічної документації на продукцію потребують корегування положення нормативно-правових актів Адміністрації Держспецзв'язку щодо їх застосування.

Означені проблеми впливають на діяльність:

громадян в частині забезпечення прав, встановлених статтями 31 та 32 Конституції України, щодо таємниці листування та захисту від втручання в особисте життя, зокрема під час взаємодії з державними органами;

державних органів, які забезпечують функціонування державної системи урядового зв'язку, державної експертизи у сфері КЗІ, електронного урядування в частині ефективного виконання покладених на них завдань;

суб'єктів господарювання - кваліфікованих надавачів електронних довірчих послуг, а саме на можливість застосування ними засобів КЕП, що відповідають вимогам законодавства у сфері електронних довірчих послуг.

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

II. Цілі державного регулювання

Проєкт Наказу розроблено з метою приведення нормативно-правових актів Адміністрації Держспецзв'язку у відповідність до вимог законодавства у сфері електронних довірчих послуг та уточнення застосування їх вимог.

III. Визначення та оцінка альтернативних способів досягнення цілей

1. Визначення альтернативних способів

Під час розробки проєкту Наказу було розглянуто такі альтернативні способи досягнення визначених цілей державного регулювання:

Вид альтернативи	Опис альтернативи
Альтернатива 1 Прийняття проєкту Наказу	Прийняття проєкту Наказу передбачає приведення нормативно-правових актів Адміністрації Держспецзв'язку у відповідність до вимог Законів України «Про електронні довірчі послуги», «Про стандартизацію», удосконалення процедур з розроблення та експертизи засобів КЗІ, шляхом затвердження змін до них.
Альтернатива 2 Відсутність регулювання	Відсутність регулювання передбачає залишення існуючого стану справ та призведе до: 1) неврегульованості процедур розроблення та експертизи засобів КЗІ, що використовуються у якості засобів УЕП та КЕП та є складовими програмно-технічних комплексів надавачів електронних довірчих послуг, та як наслідок порушень вимог Закону України «Про електронні довірчі послуги» та перешкоджанню функціонуванню інфраструктури електронних довірчих послуг; 2) залишення вразливостей функціонування державної

	системи урядового зв'язку; 3) неврегульованості питань сумісності державних електронних сервісів із форматами криптографічних протоколів, та як наслідок перешкоджанню у застосуванні цієї технології суб'єктами господарювання та населенням; 4) порушень вимог Закону України «Про стандартизацію».

2. Оцінка вибраних альтернативних способів досягнення цілей

Наразі в Україні функціонує 21 кваліфікований надавач електронних довірчих послуг, внесений центральним засвідчувальним органом до Довірчого списку, серед яких 7 не є суб'єктами господарювання.

З огляду на зазначене проєкт Наказу поширюватиметься на 14 суб'єктів господарювання.

Слід зазначити, що засоби УЕП та КЕП, також як і засоби ЕЦП, відносяться до засобів КЗІ категорії «П». Проєкт наказу не змінює порядок розроблення, виробництва та експлуатації засобів КЗІ та порядок державної експертизи у сфері КЗІ, встановлених відповідно Положенням № 141 та Положенням № 100.

Тому оцінка впливу на суб'єктів господарювання, що здійснюють діяльність з розроблення, виробництва та експлуатації засобів КЗІ не проводилася.

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	14	0	0	14
Питома вага групи у загальній кількості, відсотків	0	100	0	0	100

Вид альтернативи	Вигоди	Витрати
Альтернатива 1 Прийняття проєкту Наказу	Прийняття проєкту Наказу матиме такий вплив на інтереси суб'єктів господарювання: забезпечення використання під час надання кваліфікованих електронних довірчих послуг засобів КЕП, що мають позитивний експертний висновок за	Прийняття проєкту Наказу не призведе до збільшення витрат суб'єктів господарювання оскільки його норми спрямовані на реалізацію вимог Закону України «Про електронні довірчі послуги» без встановлення додаткових вимог.

	результатами державної експертизи у сфері КЗІ (вимога Закону України «Про електронні довірчі послуги»); підвищення попиту на послуги через підвищення рівня довіри до них, можливістю розширення функціоналу (обслуговування сертифікатів шифрування), сумісного з державними сервісами.	
Альтернатива 2 Відсутність регулювання	Відсутність регулювання означає залишення існуючого стану справ, що не передбачає жодних вигод для суб'єктів господарювання	Відсутність регулювання може призвести до додаткових перешкод у забезпеченні діяльності надавачів кваліфікованих електронних довірчих послуг у зв'язку з відсутністю на ринку достатньої кількості засобів КЕП з підтвердженою відповідністю. У зв'язку з цим витрати можуть бути пов'язанні із зменшенням прибутку або підвищенням цін на засоби КЕП (регулюється на договірних засадах) у зв'язку з підвищенням попиту на продукцію.

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

Витрати за альтернативами	Сума витрат, гривень
Альтернатива 1 Прийняття проєкту Наказу	0,00
Альтернатива 2 Відсутність регулювання	0,00

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 проєкту Наказу	4	Прийняття проєкту Наказу сприятиме: забезпеченню використання під час надання кваліфікованих електронних довірчих послуг засобів КЕП, що мають позитивний експертний висновок за результатами державної експертизи у сфері КЗІ (вимога Закону України «Про електронні довірчі послуги»); підвищенню попиту на послуги через підвищення рівня довіри до них, можливістю розширення функціоналу (обслуговування сертифікатів шифрування), сумісного з державними сервісами; підвищенню рівня надійності та захищеності електронного документообігу та електронної ідентифікації; покращенню якості надання кваліфікованих електронних довірчих послуг; підвищенню рівня довіри до кваліфікованих електронних довірчих послуг; популяризації електронного документообігу та використання засобів електронної ідентифікації
Альтернатива 2 Відсутність регулювання	1	Відсутність регулювання передбачає залишення існуючого стану справ, що спричинить додаткові перешкоди у діяльності кваліфікованих надавачів електронних довірчих послуг

Рейтинг результативності	Вигоди (підсумок)	Витрати (підсумок)	Обґрунтування відповідного місця альтернативи у рейтингу
Альтернатива 1 Прийняття проєкту Наказу	Прийняття проєкту Наказу сприятиме забезпеченню використання під час надання кваліфікованих електронних довірчих послуг засобів КЕП, що мають позитивний експертний висновок за результатами державної експертизи у сфері КЗІ (вимога Закону України «Про електронні довірчі послуги»); підвищенню попиту на послуги через підвищення рівня довіри до них, можливістю розширення функціоналу (обслуговування сертифікатів шифрування), сумісного з державними сервісами; підвищенню рівня надійності та захищеності електронного документообігу та електронної ідентифікації; покращенню якості надання кваліфікованих електронних довірчих послуг; підвищенню рівня довіри до кваліфікованих електронних довірчих послуг; популяризації	Прийняття проєкту Наказу не потребуватиме додаткового фінансування з державного бюджету, витрат суб'єктів господарювання та громадян	Продовження реформи законодавства у сфері електронного цифрового підпису з метою забезпечення належного рівня захисту інформації та персональних даних в процесі здійснення електронного документообігу та електронної ідентифікації

	електронного документообігу та використання засобів електронної ідентифікації		
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 передбачає залишення існуючого стану справ та зупинення реформи законодавства у сфері електронного цифрового підпису, що спричинить додаткові перешкоди у діяльності кваліфікованих надавачів електронних довірчих послуг	Відсутність регулювання може призвести до додаткових перешкод у забезпеченні діяльності надавачів кваліфікованих електронних довірчих послуг у зв'язку з відсутністю на ринку достатньої кількості засобів КЕП з підтвердженою відповідністю. У зв'язку з цим витрати можуть бути пов'язанні із зменшенням прибутку або підвищенням цін на засоби КЕП (регулюється на договірних засадах) у зв'язку з підвищенням попиту на продукцію.

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

Основним механізмами, які забезпечують розв'язання визначеної проблеми, є внесення змін:

1) до Положення № 141, що стосуються: поширення сфери застосування акту на засоби УЕП та КЕП (замість засобів ЕЦП); уточнення термінології; взаємоузгодження пунктів 1 та 5 розділу І; запровадження умов експлуатації засобів КЗІ за наявності документа про відповідність або позитивного експертного висновку за результатами державної експертизи у сфері КЗІ, що підтверджує клас засобу КЗІ (рівень гарантій) та реалізовані для цього методи захисту (згідно з розділом ІІ Положення № 141); встановлення особливостей розроблення, експлуатації та обліку засобів УЕП та КЕП з посиланням на відповідні нормативно-правові акти у сфері електронних довірчих послуг;

2) до Положення № 100, що стосуються: уточнення термінології, у тому числі заміни об'єкту експертизи «програмно-технічний комплекс ЦСК» на - «криптосистеми, що використовується для надання кваліфікованих електронних довірчих послуг, або в схемах електронної ідентифікації»; встановлення обов'язковості проходження державної експертизи у сфері КЗІ для засобів КЗІ, що використовуються для забезпечення функціонування державної системи урядового зв'язку; встановлення вимог до оформлення експертного висновку за результатами державної експертизи у сфері КЗІ; виключення посилань на стандарти, що втратили чинність (ДСТУ 1.3:2004, ГОСТ 2.114-95, ГОСТ 19.201-78, ГОСТ 19.202-78, ГОСТ 19.401-78, ГОСТ 19.402-78, ГОСТ 19.301-79, ГОСТ 19.503.79, ГОСТ 19.504-79, ГОСТ 19.505-79).

3) до Наказу № 739, що стосуються: звуження сфери його застосування до обсягу необхідного для забезпечення сумісності державних електронних сервісів, орієнтованих на використання кваліфікованих електронних довірчих послуг, із встановленими Вимогами № 739 форматами даних;

4) до Вимог № 739, що стосуються: уточнення термінології, виключення протоколу узгодження ключів у циклічній групі поля (оскільки стандарт ГОСТ 34.310-95 вже не застосовується в інфраструктурі відкритих ключів України);

5) до Наказу № 114, що стосуються уточнення термінології.

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

З огляду на те, що питома вага суб'єктів малого підприємництва (малих та мікропідприємств разом) у загальній кількості суб'єктів господарювання, на яких поширюється регулювання, не перевищує 10 відсотків розрахунок витрат на запровадження державного регулювання для суб'єктів малого підприємництва не проводився.

Бюджетні витрати на адміністрування регулювання для суб'єктів великого і середнього підприємництва не передбачаються.

Фінансування з державного бюджету не передбачається.

VII. Обґрунтування запропонованого строку дії регуляторного акта

Строк дії проєкту Наказу не обмежений у часі.

Зміна строку дії проєкту 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

Проєкт Наказу набирає чинності з дня його офіційного опублікування, крім пунктів 1 та 2 Змін до деяких наказів Адміністрації Державної служби спеціального зв'язку та захисту інформації України, що затверджується цим наказом, які набирають чинності через шість місяців з дня офіційного опублікування цього наказу.

VIII. Визначення показників результативності дії регуляторного акта

Показники результативності дії регуляторного акта:

кількість виданих позитивних експертних висновків за результатами державної експертизи у сфері КЗІ на засоби КЕП (оцінюватиметься через рік з дня набрання чинності проєктом Наказу);;

кількість суб'єктів господарювання, що надають послуги з обслуговування сертифікатів шифрування (оцінюватиметься через рік з дня набрання чинності проєктом Наказу);

рівень поінформованості суб'єктів господарювання та/або фізичних осіб з основних положень акта (високий, – оскільки проєкт Наказу розміщено на офіційному вебсайті Держспецзв'язку).

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 проєкту 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 в рамках державної експертизи у сфері КЗІ та від кваліфікованих надавачів електронних довірчих послуг.

Виконавець заходів з відстеження результативності проєкту Наказу – Адміністрація Держспецзв'язку.

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

«18» 09 2019 року

04/02/03-2443
24.09.2019

Повідомлення про оприлюднення
проєкту наказу Адміністрації Державної служби спеціального зв'язку та захисту інформації України «Про затвердження Змін до деяких наказів Адміністрації Державної служби спеціального зв'язку та захисту інформації України»

1. Стислий виклад змісту проєкту наказу

Проєкт наказу Адміністрації Державної служби спеціального зв'язку та захисту інформації України «Про затвердження Змін до деяких наказів Адміністрації Державної служби спеціального зв'язку та захисту інформації України», підготовлено на виконання пункту 8 розділу VII «Прикінцеві та перехідні положення» Закону України «Про електронні довірчі послуги» (далі – Закон).

Проєктом наказу пропонується привести у відповідність нормативно-правові акти Адміністрації Держспецзв'язку із Законом, зокрема в частині поширення сфери їх дії на засоби удосконаленого електронного підпису чи печатки та засоби кваліфікованого електронного підпису чи печатки замість засобів електронного цифрового підпису, узгодити їх з актами Кабінету Міністрів України прийнятими на виконання Закону, а також привести у відповідність застосування термінології відповідно до Закону.

2. Адреси для зауважень та пропозицій до проєкту акта

Адміністрація Державної служби спеціального зв'язку та захисту інформації України:

поштова: вул. Солом'янська, 13, м. Київ, 03680;

електрона: info@dsszzi.gov.ua;

Державної регуляторної служби України:

поштова: вул. Арсенальна, 9/11, м. Київ, 01011;

електрона: inform@dkrp.gov.ua.

3. Обраний спосіб оприлюднення проєкту акта

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

4. 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 **Леонід ЄВДОЧЕНКО**

«18» 09 2019 року

Пр и 04102/03-2744

Прим. № __

ПРОТОКОЛ УЗГОДЖЕННЯ ПОЗИЦІЙ

до проєкту наказу Адміністрації Держспецзв'язку «Про затвердження Змін до деяких наказів Адміністрації Державної служби спеціального зв'язку та захисту інформації України»

1. Неврегульовані розбіжності

Редакція спірної частини проєкту акта	**Найменування органу виконавчої влади, що подав зауваження (пропозиції) та їх зміст**	**Мотиви відхилення зауважень (пропозицій) розробником**
Пропозиції до пункту 1 Змін (Положення про порядок розроблення, виробництва та експлуатації засобів криптографічного захисту інформації, затверджене наказом Адміністрації Держспецзв'язку від 20.07.2007 року № 141)		
1) у розділі I: пункт 1 викласти у такій редакції: «1. Це Положення визначає вимоги до порядку розроблення, виробництва та експлуатації засобів криптографічного захисту державних інформаційних ресурсів або інформації, вимога щодо захисту якої встановлена законом, **засобів удосконаленого електронного підпису чи печатки**, засобів кваліфікованого електронного підпису чи печатки, засобів, спеціально призначених для розроблення, дослідження, виробництва та випробування засобів криптографічного захисту інформації (далі – засоби КЗІ). Особливості розроблення, виготовлення, уведення в експлуатацію та експлуатації засобів КЗІ, призначених для криптографічного захисту інформації, що становить державну таємницю, та службової інформації визначаються відповідно до чинного законодавства. Розроблення засобів КЗІ, що фінансується за рахунок коштів Державного	**Національний банк України** Виключити норми, що стосуються засобів удосконаленого електронного підпису чи печатки, оскільки Законом України «Про електронні довірчі послуги» наявність документа про підтвердження відповідності або позитивного експертного висновку за результатами державної експертизи у сфері криптографічного захисту інформації передбачена тільки для засобів кваліфікованого електронного підпису чи печатки.	Відповідно до частини першої статті 1 Закону України «Про електронні довірчі послуги» (далі – Закон) засіб удосконаленого електронного підпису чи печатки - апаратно-програмний або апаратний пристрій чи програмне забезпечення, які реалізують криптографічні алгоритми генерації пар ключів та/або створення удосконаленого електронного підпису чи печатки, та/або перевірки удосконаленого електронного підпису чи печатки, та/або зберігання особистого ключа удосконаленого електронного підпису чи печатки. Частиною третьою статті 14 Закону встановлено, що використання удосконалених електронних підписів та печаток забезпечує середній рівень довіри до схем електронної ідентифікації. Частиною другою статті 14 Закону встановлено, що середній рівень довіри до засобів електронної ідентифікації повинен характеризувати засоби електронної ідентифікації в контексті схеми електронної ідентифікації, яка забезпечує суттєвий ступінь

бюджету України, погоджується з Адміністрацією Державної служби спеціального зв'язку та захисту інформації України (далі - Адміністрація Держспецзв'язку). Національний банк України може розробляти засоби КЗІ, призначені виключно для забезпечення власних потреб та потреб банківської системи України, без погодження з Адміністрацією Держспецзв'язку.»; у пункті 2 слова «надійних засобів електронного цифрового підпису та засобів, спеціально призначених для розроблення, дослідження, виробництва та випробування засобів КЗІ» виключити;		довіри до заявлених або затверджених ідентифікаційних даних і описується з посиланням на технічні специфікації, стандарти і процедури, що до неї відносяться, включаючи технічні засоби контролю, призначенням яких є істотне зниження ризику зловживання або спростування ідентичності. Тому засоби удосконаленого електронного підпису чи печатки повинні мати характеристики, що відповідають елементам технічних специфікацій та процедур, наведених у додатку 2 Вимог 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 України 27.11.2018 № 86, та зареєстрованих Мін'юстом 26.12.2018 за № 1462/32914. Відповідно до частини третьої статті 26 Закону до кваліфікованої електронної позначки часу додається створений для неї удосконалений електронний підпис чи удосконалена електронна печатка. Таким чином засіб удосконаленого електронного підпису чи печатки є засобом КЗІ, який може використовуватися в рамках надання кваліфікованої електронної довірчої послуги формування, перевірки та підтвердження кваліфікованої електронної позначки часу та електронних довірчих послуг, які забезпечують середній рівень довіри до схем електронної ідентифікації, та призначений для захисту інформації

		(особистих ключів), вимога щодо захисту якої встановлена Законом. Тому поширення вимог Положення про порядок розроблення, виробництва та експлуатації засобів криптографічного захисту інформації, затвердженого наказом Адміністрації Держспецзв'язку від 20.07.2007 року № 141, на засоби удосконаленого електронного підпису чи печатки є обов'язковим.
3) у розділі IV: пункт 1 викласти у такій редакції: «1. Для криптографічного захисту державних інформаційних ресурсів або інформації, вимога щодо захисту якої встановлена законом, використовуються засоби КЗІ, які мають **документ про відповідність** або позитивний експертний висновок за результатами державної експертизи у сфері КЗІ, що підтверджують клас засобу КЗІ (рівень гарантій) та реалізовані методи захисту, а суб'єкти, що їх використовують, мають на це права. **Оцінка відповідності** та державна експертиза у сфері криптографічного захисту інформації проводяться в порядку, визначеному відповідними нормативно-правовими актами.»;	**Міністерство економічного розвитку і торгівлі України** Відповідно до статті 25 Закону України «Про технічні регламенти та оцінку відповідності» оцінка відповідності вимогам технічних регламентів здійснюється у випадках і шляхом застосування процедур оцінки відповідності, які визначені в таких технічних регламентах. Згідно з частиною четвертою статті 9 Закону технічні регламенти затверджуються законами, актами Кабінету Міністрів України та центральних органів виконавчої влади. Технічні регламенти, якими передбачене застосування процедур оцінки відповідності, затверджуються законами або актами Кабінету Міністрів України. На сьогодні в Україні відсутній технічний регламент, яким передбачено застосування процедур оцінки відповідності засобів криптографічного захисту інформації. Ураховуючи зазначене, абзац четвертий підпункту 3 пункту 1 Змін пропонуємо доопрацювати, виключивши положення щодо здійснення оцінки відповідності засобів	Необхідність застосування процедур оцінки відповідності у сфері КЗІ визначена законодавством. Частиною третьою статті 19 Закону України «Про електронні довірчі послуги» встановлено, що відповідність засобів кваліфікованого електронного підпису чи печатки зазначеним вимогам підтверджується **документами про відповідність** або позитивними експертними висновками за результатами їх державної експертизи у сфері криптографічного захисту інформації. Відповідно до пункту 8 Положення про порядок здійснення криптографічного захисту інформації, затвердженого пунктом 8 Указу Президента України від 22 травня 1998 року № 505/98, для криптографічного захисту конфіденційної інформації використовуються криптосистеми і засоби криптографічного захисту, які мають **сертифікат відповідності**.

	криптографічного захисту інформації.	
Норма відсутня Витяг з Положення про порядок розроблення, виробництва та експлуатації засобів криптографічного захисту інформації, затвердженого наказом Адміністрації Держспецзв'язку від 20 липня 2007 року № 141: *12. У засобах КЗІ використовуються криптоалгоритми та криптопротоколи, які є національними стандартами, або ті, на які за результатами експертних досліджень Адміністрацією Держспецзв'язку видано позитивний експертний висновок.* ***Інші криптоалгоритми та криптопротоколи для використання виключно в банківській системі України погоджуються Адміністрацією Держспецзв'язку за відповідним зверненням та обґрунтуванням Національного банку України***	**Національний банк України** Внести зміни до пункту 12 розділу II діючого Положення про порядок розроблення, виробництва та експлуатації засобів криптографічного захисту інформації, затвердженому наказом Адміністрації Держспецзв'язку від 20 липня 2007 року № 141, виклавши абзац перший у новій редакції: «У засобах КЗІ використовуються криптоалгоритми та криптопротоколи, які є національними стандартами, або ті, на які за результатами експертних досліджень Адміністрації Держспецзв'язку видано позитивний експертний висновок, **або криптоалгоритми та криптопротоколи, реалізовані у складових частинах апаратури чи програмного забезпечення, які мають в наявності чинний документ про підтвердження відповідності міжнародному стандарту ISO/IEC 15408, виданий акредитованим органом країни-члена ЄС»**	Пропозиції не стосуються положень проєкту акту Реалізацію пропозицій у іншому проєкті акту вважаємо не доцільним, оскільки норма, до якої надано пропозиції спрямована унормувати питання реалізації у засобах КЗІ оцінених криптоалгоритмів або криптопротоколів, а не комплектування засобу КЗІ певною апаратурою чи програмним забезпеченням. Процедури оцінки криптостійкості криптоалгоритму та оцінки відповідності засобів КЗІ (складових частин апаратури чи програмного забезпечення) є різними. Так, реалізація в засобі певного алгоритму та оцінка відповідності засобу КЗІ міжнародному стандарту ISO/IEC 15408 не дає відповіді щодо стійкості криптографічного алгоритму (реалізованого в цьому засобі).
Норма відсутня	**Міністерство економічного розвитку і торгівлі України** Частинами першою та другою статті 23 Закону України «Про стандартизацію» визначено, що національні стандарти та кодекси усталеної практики застосовуються безпосередньо чи шляхом посилання на них в інших документах. Національні стандарти та кодекси усталеної практики застосовуються на добровільній основі, крім випадків, якщо	Пропозиції не стосуються положень проєкту акту Пропозиції стосуються зміни процедур розроблення та виробництва засобів КЗІ та потребують додаткового вивчення, сумісного обговорення та відстеження їх результативності у разі їх запровадження іншим проєктом акту. **Слід зазначити, що діюча процедура розроблення засобів КЗІ передбачає**

	обов'язковість їх застосування встановлена нормативно-правовими актами. Ураховуючи зазначене, нормативно-правові акти не повинні містити положень, які передбачають, що продукція, процеси, послуги мають виготовлятись, проводитись, надаватись відповідно до національних стандартів без наведення позначень відповідних національних стандартів. З огляду на викладене, пропонуємо внести зміни до діючого Положення про порядок розроблення, виробництва та експлуатації засобів криптографічного захисту інформації, затвердженому наказом Адміністрації Держспецзв'язку від 20 липня 2007 року № 141 (далі – Положення № 141)	**добровільне застосування національних стандартів розробником засобів КЗІ, що задовільняє вимогам ТЗ (документ розробника), у достатньому обсязі (перевіряється Держспецзв'язку в рамках погодження ТЗ для оцінки відповідності вимог до засобу КЗІ для віднесення його до певного класу). Застосування стандартизованих рішень забезпечує певну якість продукції (криптографічну стійкість тощо) навіть без посилань на конкретні стандарти.** Розроблення засобів КЗІ без застосування тих чи інших стандартів у сфері КЗІ (на вибір розробника або відповідно до законодавства) практично є неможливим.
Витяг з Положення про порядок розроблення, виробництва та експлуатації засобів криптографічного захисту інформації, затвердженого наказом Адміністрації Держспецзв'язку від 20 липня 2007 року № 141: *«II. Розроблення засобів КЗІ* *10. До ТЗ на ДКР з розроблення нового типу або модернізації існуючого зразка засобу КЗІ вносяться:* ... *перелік нормативно-правових актів, **нормативних** та інших документів, які містять вимоги та положення щодо розроблення або модернізації існуючого зразка засобу КЗІ;* ... *12. У засобах КЗІ використовуються криптоалгоритми та криптопротоколи, **які є національними стандартами, або ті**, на які за результатами експертних досліджень Адміністрацією Держспецзв'язку видано	У розділі II: в абзаці тринадцятому пункту 10 слова «, нормативних» виключити; в абзаці першому пункту 12 слова «, які є національними стандартами, або ті» виключити;	Тлумачення Мінекономрозвитку (*нормативно-правові акти не повинні містити положень, які передбачають, що продукція, процеси, послуги мають виготовлятись, проводитись, надаватись відповідно до національних стандартів без наведення позначень відповідних національних стандартів*) не повною мірою узгоджується з нормами статті 23 Закону України «Про стандартизацію», статтею 1 Закону України «Про технічні регламенти та оцінку відповідності», статтею 3 Закону України «Про наукову і науково-технічну експертизу». Так, у статті 23 Закону про стандартизацію відсутні норми про заборону встановлення нормативно-правовими актами загальних вимог щодо відповідності продукції національним стандартам без наведення

позитивний експертний висновок. Інші криптоалгоритми та криптопротоколи для використання виключно в банківській системі України погоджуються Адміністрацією Держспецзв'язку за відповідним зверненням та обґрунтуванням Національного банку України. *14. У засобах КЗІ повинні бути реалізовані методи захисту, що відповідають установленим вимогам, залежно від виду, типу, категорії, класу засобу КЗІ.* *...* *Вимоги для засобів КЗІ категорії «Р» визначаються з урахуванням вимог* ***нормативних документів*** *системи технічного захисту інформації.*	в абзаці одинадцятому пункту 14 слова «нормативних документів» замінити словами нормативно-правових актів»;	позначень відповідних національних стандартів. Відповідно до статті 1 Закону України «Про технічні регламенти та оцінку відповідності» під оцінкою відповідності продукції розуміється процес доведення того, що **задані вимоги**, які стосуються продукції, процесу, послуги, системи, особи чи органу, були виконані. В той же час під **заданими вимогами** розуміється заявлені потреби чи очікування, які зафіксовані в технічних регламентах, **стандартах**, технічних специфікаціях або в інший спосіб.
17. Розробник розробляє робочу конструкторську документацію на засіб КЗІ, до складу якої обов'язково входять ***проект технічних умов (для апаратних та апаратно-програмних засобів КЗІ, що виготовляються серійно)****, експлуатаційні документи, інструкція із забезпечення безпеки експлуатації засобу КЗІ та інструкція щодо порядку генерації ключових даних і поводження (облік, зберігання, знищення) з ключовими документами (обов'язково для засобів КЗІ видів А та Б, підвидів Б1 та Б2), а також інструкцію про порядок застосування виробу в складі засобу КЗІ виду А або Б, підвидів Б1 та Б2 (для засобів КЗІ виду В).*	у пункті 17:	
	в абзаці першому слова «проект технічних умов (для апаратних та апаратно-програмних засобів КЗІ, що виготовляються серійно),» виключити;	
Технічні умови на програмні засоби КЗІ можуть не розроблятися.	абзац другий виключити;	
18. Проект технічних умов (далі - ТУ) погоджується з Адміністрацією	пункт 18 виключити;	

Держспецзв'язку. За потреби розробником до ТУ вноситься перелік допустимих змін, які без погодження з Адміністрацією Держспецзв'язку можуть уноситися під час виробництва засобу КЗІ до його конструкції, схемотехнічних рішень, програмного забезпечення та переліку комплектувальних виробів тощо. У цьому разі до проекту ТУ, що подається на погодження, додається пояснювальна записка з обґрунтуванням можливості внесення відповідних змін без впливу на криптографічні та спеціальні якості засобів КЗІ. У разі визначення в технічному завданні вимог щодо захисту засобу КЗІ від витоку інформації каналами ПЕМВН у ТУ наводяться посилання на методику контролю спеціальних показників в умовах серійного виробництва засобів КЗІ, яка має бути узгоджена з організацією, що здійснює сертифікаційні випробування (експертні роботи), та Адміністрацією Держспецзв'язку *ІІІ. Виробництво засобів КЗІ* *1. Виробництво засобів КЗІ здійснюється тільки за наявності чинного сертифіката відповідності (позитивного експертного висновку) на засіб КЗІ та на засоби (комплекси), призначені для розроблення, дослідження, виробництва та випробувань засобів КЗІ (у разі його використання), **ТУ** та інструкції із забезпечення безпеки експлуатації засобів КЗІ.* *2. Виробники засобів КЗІ повинні:* *ужити заходів щодо своєчасної сертифікації або експертизи засобів КЗІ (у*	у розділі ІІІ: у пункті 1 слова «, ТУ» виключити;	

тому числі повторної - після закінчення строку дії раніше отриманого сертифіката відповідності або експертного висновку); *погодити зміни, які вносяться у вироби та документацію на них, із замовником та Адміністрацією Держспецзв'язку;* ***забезпечити виконання усіх вимог ТУ;*** *з усієї партії виробів, що виготовляється, вибрати контрольний еталонний зразок та зберігати його відповідно до встановлених вимог* ***(за наявності таких вимог у ТУ)****;* *забезпечити технічне обслуговування та гарантійний ремонт засобів КЗІ, а також випуск і постачання запасних частин для цих засобів відповідно до Закону України «Про захист прав споживачів».*	у пункті 2: абзац четвертий виключити; у абзаці п'ятому слова «(за наявності таких вимог у ТУ)» виключити.	
Пропозиції до пункту 2 Змін (Положення про державну експертизу в сфері криптографічного захисту інформації, затверджене наказом Адміністрації Держспецзв'язку від 23.06.2008 № 100)		
1) у розділі I: … абзац п'ятий пункту 1.6 викласти в такій редакції: «криптосистеми, засоби й обладнання криптографічного захисту державних інформаційних ресурсів або інформації, вимога щодо захисту якої встановлена законом, **криптосистеми, що використовуються для надання кваліфікованих електронних довірчих послуг, або в схемах електронної ідентифікації, засоби удосконаленого електронного підпису чи печатки**, засоби кваліфікованого електронного підпису чи	**Національний банк України** 1. Виключити норми, що стосуються засобів удосконаленого електронного підпису чи печатки, оскільки Законом України «Про електронні довірчі послуги» наявність документа про підтвердження відповідності або позитивного експертного висновку за результатами державної експертизи у сфері криптографічного захисту інформації передбачена тільки для засобів кваліфікованого електронного підпису чи печатки 2. З урахуванням визначених статтею 15 Закону України «Про електронні довірчі послуги» схем електронної ідентифікації та	Обґрунтування ідентичне обґрунтуванню Адміністрації Держспецзв'язку наведеному до зауважень Національного банку до пункту 1 Змін

печатки;»; пункт 1.6 доповнити абзацами шість та сім такого змісту: «засоби, що реалізують криптоперетворення та/або механізми імітозахисту, та використовуються в системах зв'язку, управління та озброєння; засоби обробки та передачі державних інформаційних ресурсів або інформації, вимога щодо захисту якої встановлена законом, які реалізують функції криптографічного захисту інформації;». 2) у абзаці четвертому підпункту 2.1.1 пункту 2.1 розділу II слова «програмно-технічні комплекси центрів сертифікації ключів, які передбачають акредитацію, надійні засоби електронного цифрового підпису» замінити словами «**засоби удосконаленого електронного підпису чи печатки**, засоби кваліфікованого електронного підпису чи печатки».	встановлених рівнів довіри до засобів електронної ідентифікації, що використовуються в цих схемах електронної ідентифікації, пропонуємо встановити, що обов'язковій експертизі підлягають тільки криптосистеми, які використовуються в схемах електронної ідентифікації з високим рівнем довіри.	
Норма відсутня	**Міністерство економічного розвитку і торгівлі України** Частинами першою та другою статті 23 Закону про стандартизацію визначено, що національні стандарти та кодекси усталеної практики застосовуються безпосередньо чи шляхом посилання на них в інших документах. Національні стандарти та кодекси усталеної практики застосовуються на добровільній основі, крім випадків, якщо обов'язковість їх застосування встановлена нормативно-правовими актами. Ураховуючи зазначене, нормативно-	Пропозиції не стосуються положень проєкту акту Обґрунтування ідентичне обґрунтуванню Адміністрації Держспецзв'язку наведеному до зауважень Мінекономрозвитку до пункту 1 Змін

Витяг з Положення про державну експертизу в сфері криптографічного захисту інформації, затверджене наказом Адміністрації Держспецзв'язку від 23.06.2008 № 100: «*І. Загальні положення* *1.3. Використані в цьому Положенні терміни вживаються в такому значенні:* *державна експертиза у сфері КЗІ (далі - експертиза) - діяльність, метою якої є визначення за результатами аналізу матеріалів експертних (тематичних) досліджень відповідності об'єктів експертизи вимогам* ***нормативних документів та (або)*** *нормативно-правових актів у сфері КЗІ, оцінка рівня та механізмів захисту інформації об'єктом експертизи або науково-технічного рівня об'єкта експертизи, підготовка обґрунтованих висновків і надання рекомендацій для прийняття рішення про використання (застосування) об'єкта експертизи за призначенням;* *експертні дослідження – дослідження та аналіз конкретних властивостей засобів криптографічного захисту інформації, криптографічних алгоритмів, засобів, систем та комплексів спеціального зв'язку з метою перевірки їх відповідності вимогам*	правові акти не повинні містити положень, які передбачають, що продукція, процеси, послуги мають виготовлятись, проводитись, надаватись відповідно до національних стандартів без наведення позначень відповідних національних стандартів. З огляду на викладене, пропонуємо внести зміни до діючого Положення про державну експертизу в сфері криптографічного захисту інформації, затвердженому наказом Адміністрації Держспецзв'язку від 23 червня 2008 року № 100: у розділі І: у пункті 1.3: в абзаці третьому слова «нормативних документів та(або)» виключити; в абзаці п'ятому та десятому слова «нормативних документів та/або» виключити;	

нормативних документів та/або *нормативно-правових актів, оцінки захищеності інформації або їх науковотехнічного рівня;* *тематичні дослідження – дослідження щодо встановлення відповідності засобів криптографічного захисту інформації, криптосистем, криптографічних алгоритмів, засобів, систем і комплексів спеціального зв'язку, які призначені для захисту інформації, що становить державну таємницю, або службової інформації вимогам тактико-технічних завдань на їх створення,* ***нормативних документів та/або*** *нормативно-правових актів у сфері криптографічного захисту інформації, а також вимогам із захисту від витоку інформації каналами побічних електромагнітних випромінювань і наведень.* *1.6. Експертиза є обов'язковою або добровільною. Обов'язковій експертизі підлягають:* *засоби та методи, призначені для розробки, дослідження, виробництва та випробувань засобів криптографічного захисту державних інформаційних ресурсів або інформації, вимога щодо захисту якої встановлена законом;* *криптографічні алгоритми та криптографічні протоколи, які планується визначити як такі, що рекомендовані для використання або* ***як національні стандарти****;* …	в абзаці третьому пункту 1.6 слова «або як національні стандарти» виключити;	

1.13. Основними завданнями Експертної комісії є: *аналіз стану та розробка пропозицій щодо вдосконалення методології проведення експертних (тематичних) досліджень і процедур проведення експертизи їх результатів;*	у пункті 1.13:	
формування та розгляд пропозицій щодо розробки та вдосконалення нормативно-правових актів ***і нормативних документів*** *з питань організації та проведення експертизи;*	в абзаці третьому слова «і нормативних документів» виключити;	
...		
підготовка пропозицій щодо погодження (затвердження) ***нормативної та*** *технічної документації, що регламентує використання об'єктів експертизи;*	в абзаці восьмому слова «нормативної та» виключити;	
II. Порядок організації та проведення експертизи *2.1. Подання та розгляд заявки, укладання договорів*	у розділі II:	
2.1.1. Для проведення експертизи таких об'єктів, як:		
У складі комплекту документів на проведення державної експертизи криптографічних засобів вітчизняного виробництва, які виготовляються серійно, обов'язково подаються технічні умови, затверджені та зареєстровані в установленому порядку. ***Для криптографічних засобів***	абзаци шостий та сьомий підпункту 2.1.1 пункту 2.1 виключити;	

вітчизняного виробництва, які заплановано виготовляти серійно та які вперше подані на державну експертизу, подається погоджений замовником розробки криптографічного засобу проект технічних умов. За позитивними результатами державної експертизи проект технічних умов погоджується Адміністрацією Держспецзв'язку.		
2.1.14. ...		
Якщо зміни у законодавстві вимагають унесення змін до технічних умов на криптографічний засіб, замовник експертизи інформує про це Адміністрацію Держспецзв'язку та повторно подає заявку після унесення цих змін.	абзац третій підпункту 2.1.14 пункту 2.1 виключити;	
2.3.13. Термін дії експертного висновку визначається з урахуванням криптографічних якостей криптографічного засобу, ***терміну дії нормативних документів****, умов та граничного терміну експлуатації криптографічного засобу, але не більше термінів, зазначених у додатку 5 до цього Положення.*	у пункті 2.3.13 пункту 2.3 слова «терміну дії нормативних документів,» виключити;	
2.3.14. Експертний висновок може бути виданий на один зразок криптографічного засобу, партію засобів, а також засіб, що виробляється серійно, ***за наявності технічних умов на нього.***	у підпункті 2.3.14 пункту 2.3: в абзаці першому слова «, за наявності технічних умов на нього» виключити;	
На програмний криптографічний засіб, зазначений в абзаці сьомому підпункту 2.1.1 пункту 2.1 цього розділу, який виготовляється серійно, видається	абзац другий виключити;	

експертний висновок за відсутності технічних умов.		
2.3.19. У разі виникнення необхідності внесення змін до об'єкта експертизи або в ***нормативні та*** *інші документи на об'єкт експертизи, зміни технології виробництва криптографічних засобів замовник повинен письмово сповістити про це Адміністрацію Держспецзв'язку та надати відповідні матеріали з пояснювальною запискою щодо обґрунтування впливу змін на якості об'єкта експертизи. Адміністрація Держспецзв'язку за результатами аналізу наданих замовником матеріалів приймає рішення щодо надання дозволу на внесення змін або необхідності проведення експертизи. Про прийняте рішення Адміністрація Держспецзв'язку повідомляє замовника протягом місяця з дня отримання його повідомлення.*	у пункті 2.3.19 пункту 2.3 слова «нормативні та» виключити;	
додаток 3 до Положення № 100: (Перелік документів та матеріалів, необхідних для проведення експертизи криптографічних засобів іноземного виробництва)	у додатку 3 до Положення про державну експертизу:	
2. Документ виробника про гарантії та відповідність криптографічних засобів вимогам чинних ***нормативних документів****.*	у пункті 2 слова «чинних нормативних документів» замінити словами «нормативно-правових актів»;	
6. Нормативні документи (стандарти, технічні умови, специфікації тощо), які встановлюють вимоги до криптографічних засобів.	пункт 6 виключити;	
додаток 7 до Положення № 100: (Акт відбору зразків для проведення державної	у додатку 7 до Положення про державну	

експертизи в сфері криптографічного захисту інформації) *Під час відбору встановлено:* *наявність (відсутність) технічного завдання **або технічних умов**;* *найменування зразків відповідають (не відповідають) наведеним у технічному завданні, **технічних умовах** або заявці найменуванням;* *комплектність зразків відповідає (не відповідає) технічному завданню, **технічним умовам**;* *серійні номери зразків відповідають (не відповідають) номерам, які зазначені в документації зразків.»*	експертизу: в абзаці дев'ятому слова «або технічних умов» виключити; в абзаці десятому слова «, технічних умов» виключити; в абзаці одинадцятому слова «, технічним умовам» виключити.	
Пропозиції до пункту 3 Змін **(Наказ Адміністрації Державної служби спеціального зв'язку та захисту інформації України від 18.12.2012 року № 739)**		
пункт 3 викласти у такій редакції: «3. Установити, що кваліфіковані надавачі електронних довірчих послуг мають право надавати послуги з обслуговування сертифікатів шифрування, та у разі фактичного їх надання інформують про це Адміністрацію Держспецзв'язку.»;	**Національний банк України** Пропонуємо виключити норму про обов'язок кваліфікованих надавачів електронних довірчих послуг інформувати Адміністрацію Держспецзв'язку про факт надання послуг з обслуговування сертифікатів шифрування або надати відповідні обґрунтування у пояснювальній записці	Відповідно до пункту 2) частини першої статті 14, пункту 1) частини першої статті 15 Закону України «Про Державну службу спеціального зв'язку та захисту інформації України» (далі – Закон про Держспецзв'язку) Держспецзв'язку приймає участь у формуванні та реалізації державної політики у сферах електронного документообігу (в частині захисту інформації державних органів та органів місцевого самоврядування) та має право одержувати в установленому порядку від органів державної влади, органів місцевого самоврядування, військових формувань, утворених відповідно до законів України, підприємств, установ і організацій незалежно від форми власності

		інформацію, документи і матеріали, необхідні для виконання покладених на Державну службу спеціального зв'язку та захисту інформації України завдань.
Пропозиції до пункту 4 Змін (Вимоги до форматів криптографічних повідомлень, затверджені наказом Адміністрації Держспецзв'язку від 18.12.2012 № 739)		
1) у розділі I: у пункті 1.1 слова «та надійних засобів електронного цифрового підпису (далі – ЕЦП)» виключити; пункт 1.2 викласти у такій редакції: «1.2. Положення цих Вимог є обов'язковими для засобів КЗІ, призначених для забезпечення конфіденційності інформації з використанням сертифіката шифрування. Правильність реалізації у засобах КЗІ цих Вимог повинна бути підтверджена **документом про відповідність** або позитивним експертним висновком за результатами державної експертизи у сфері КЗІ. **Оцінка відповідності та** державна експертиза у сфері КЗІ проводяться в порядку, визначеному відповідними нормативно-правовими актами.»;	**Міністерство економічного розвитку і торгівлі України** Відповідно до статті 25 Закону України «Про технічні регламенти та оцінку відповідності» оцінка відповідності вимогам технічних регламентів здійснюється у випадках і шляхом застосування процедур оцінки відповідності, які визначені **в таких технічних регламентах**. Згідно з частиною четвертою статті 9 Закону технічні регламенти затверджуються законами, актами Кабінету Міністрів України та центральних органів виконавчої влади. Технічні регламенти, якими передбачене застосування процедур оцінки відповідності, затверджуються законами або актами Кабінету Міністрів України. На сьогодні в Україні відсутній технічний регламент, яким передбачено застосування процедур оцінки відповідності засобів криптографічного захисту інформації. Ураховуючи зазначене, абзац п'ятий підпункту 1 пункту 4 проекту Змін пропонуємо доопрацювати, виключивши положення щодо здійснення оцінки відповідності засобів криптографічного захисту інформації.	Обґрунтування ідентичне обґрунтуванню Адміністрації Держспецзв'язку наведеному до зауважень Мінекономрозвитку до пункту 1 Змін

5) у розділі V: …. у главі 6: пункт 6.3 виключити; пункт 6.4 вважати пунктом 6.3; у пункті 6.3: підпункт 1 викласти у такій редакції: «1) KDF-функція в групі точок еліптичної кривої (ECDH) ґрунтується на ДСТУ ISO/IEC 11770-3:2015.»;	**Міністерство економічного розвитку і торгівлі України** В позиції 1 пункту 6.4 глави 6 розділу V слова «ДСТУ ISO/IEC 15946-3:2002» замінити словами «ДСТУ ISO/IEC 15946-3:2006»	Враховуючи скасування міжнародного стандарту ISO/IEC 15946-3, застосування відповідного йому ДСТУ ISO/IEC 15946-3:2006 не вбачається. Замість цього використовується чинний та гармонізований в Україні ДСТУ ISO/IEC 11770-3:2015 в якому визначено протокол узгодження ключа Діффі-Гелмана.
Норма відсутня	**Міністерство економічного розвитку і торгівлі України** У тексті вимог посилання на ДСТУ ГОСТ 28147:2009 необхідно виключити	На цей час ДСТУ ГОСТ 28147:2009 масово реалізується у засобах КЗІ та застосовується у складі криптографічного комплекту ДСТУ 4145-2002, ГОСТ 34.311-95 та ДСТУ ГОСТ 28147:2009 (далі – криптокомплект) для накладання цифрового підпису. Враховуючи це, а також організаційно-технічні заходи необхідні для впровадження нового альтернативного алгоритму згідно ДСТУ 7564:2014 передбачено такий перехідний період у застосуванні ДСТУ ГОСТ 28147:2009: до 01.01.2022 у будь-яких засобах КЗІ, у тому числі для накладення цифрового підпису у складі криптокомплекту; без обмежень у часі для перевірки цифрового підпису у складі криптокомплекту.

Пропозиції до пункту 5 Змін (Інструкція про порядок постачання і використання ключів до засобів криптографічного захисту інформації, затверджена наказом Адміністрації Держспецзв'язку від 12.06.2007 року № 114		
5. У Інструкції про порядок постачання і використання ключів до засобів криптографічного захисту інформації, затвердженій наказом Адміністрації Державної служби спеціального зв'язку та захисту інформації України від 12 червня 2007 року № 114, зареєстрованій в Міністерстві юстиції України 25 червня 2007 року за № 729/13996 (зі змінами): у пункті 1.1 слова «електронний цифровий підпис» замінити словами «електронні довірчі послуги»; у пункті 1.2 абревіатуру, символ та цифри «ГОСТ 28147 89» замінити абревіатурами, символом та цифрами «**ДСТУ ГОСТ 28147:2009**».	**Міністерство економічного розвитку і торгівлі України** Абзац третій пункту 5 проекту Змін пропонуємо викласти у такій редакції: «у пункті 1.2 слова «ГОСТ 28147-89 «Системы обработки информации. Защита криптографическая. Алгоритм криптографического преобразования» (далі - ГОСТ 28147-89) замінити словами Адміністрацією Державної служби спеціального зв'язку та захисту інформації України	Обґрунтування ідентичне обґрунтуванню Адміністрації Держспецзв'язку наведеному до зауважень Мінекономрозвитку до пунктів 1 та 4 Змін
Норма відсутня Витяг з Інструкції про порядок постачання і використання ключів до засобів криптографічного захисту інформації, затверджена наказом Адміністрації Держспецзв'язку від 12.06.2007 № 114: *«2.6. Генерація РК у засобах КЗІ повинна здійснюватися відповідно **до національних стандартів** або за методикою генерації ключів, яка погоджується встановленим порядком на підставі результатів державної експертизи у сфері КЗІ.* *2.7. Ключі можуть розподілятися між засобами КЗІ каналами (лініями) зв'язку в*	**Міністерство економічного розвитку і торгівлі України** У пунктах 2.6, 2.7 та 2.9 глави 2 діючої Інструкції про порядок постачання і використання ключів до засобів криптографічного захисту інформації слова «національних стандартів» замінити словами «Нормативно-правових актів».	Пропозиції не стосуються положень проєкту акту Обґрунтування ідентичне обґрунтуванню Адміністрації Держспецзв'язку наведеному до зауважень Мінекономрозвитку до пункту 1 Змін

захищеному вигляді. Розподіл ключів повинен здійснюватися відповідно ***до національних стандартів*** *або за методикою розподілу ключів, погодженою встановленим порядком на підставі результатів державної експертизи у сфері КЗІ.* *2.9. Термін дії ДКЕ, наведених у додатку 1 до цієї Інструкції, а також термін дії РК, генерація яких здійснена відповідно до* ***національних стандартів****, визначається замовником.»*		

2. Враховані зауваження (пропозиції)

Редакція частини проекту акта, до якої висловлено зауваження (пропозиції)	Найменування органу виконавчої влади, що подав зауваження (пропозиції) та їх зміст	Спосіб врахування
Проєкт наказу Адміністрації Держспецзв'язку «Про затвердження Змін до деяких наказів Адміністрації Державної служби спеціального зв'язку та захисту інформації України»		
Відповідно до 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, **та з метою удосконалення законодавства у сфері електронного цифрового підпису**	**Державне агентство з питань електронного урядування** Преамбула проекту акта не враховує вимоги Закону України «Про електронні довірчі послуги», зокрема статті 1. У проекті акта слова «у сфері електронного цифрового підпису» необхідно замінити на слова «у сфері електронних довірчих послуг»	Відповідно до 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, **та з метою удосконалення нормативно-правових актів у сфері криптографічного захисту інформації та приведення їх у відповідність до законодавства**
4. Цей наказ набирає чинності з дня його офіційного опублікування.	**Міністерство економічного розвитку і торгівлі України** Частиною другою статті 19 Закону України «Про технічні регламенти та оцінку відповідності» встановлено, що нормативно-правові акти, якими затверджуються технічні регламенти і процедури оцінки відповідності	4. Цей наказ набирає чинності з дня його офіційного опублікування, крім пунктів 1 та 2 Змін до деяких наказів Адміністрації Державної служби спеціального зв'язку та захисту інформації України, що затверджується цим наказом, які набирають чинності через шість місяців з дня

	або вносяться зміни до них, за винятком нормативно-правових актів, прийнятих за невідкладних обставин, що визначені статтею 18 цього Закону (у сфері захисту життя чи здоров'я людей, тварин або рослин, охорони довкілля чи природних ресурсів або національної безпеки), набирають чинності у термін, визначений цими нормативно-правовими актами, але не раніше ніж через шість місяців з дня їх офіційного опублікування, з метою надання суб'єктам господарювання часу для приведення своєї продукції або пов'язаних з нею процесів чи методів виробництва відповідно до нових вимог. Відповідно до частини другої статті 21 Закону України «Про технічні регламенти та оцінку відповідності» прийняті зміни до технічних регламентів і процедур оцінки відповідності опубліковуються та набирають чинності відповідно до статті 19 цього Закону. Отже, пункт 4 проекту наказу пропонуємо викласти у такій редакції «4. Цей наказ набирає чинності з дня його офіційного опублікування, крім пункту 1 Змін до деяких наказів Адміністрації Державної служби спеціального зв'язку та захисту інформації України, що затверджується цим наказом, який набирає чинності через шість місяців з дня офіційного опублікування цього наказу.»	офіційного опублікування цього наказу.
Пропозиції до пункту 1 Змін (Положення про порядок розроблення, виробництва та експлуатації засобів криптографічного захисту інформації, затверджене наказом Адміністрації Держспецзв'язку від 20.07.2007 року № 141)		
Норма відсутня	**Міністерство економічного розвитку і торгівлі України**	2) у розділі II: пункт 1 викласти у такій редакції: «1. Розроблення засобів КЗІ

	Пропонуємо внести зміни до діючого Положення про порядок розроблення, виробництва та експлуатації засобів криптографічного захисту інформації, затвердженому наказом Адміністрації Держспецзв'язку від 20 липня 2007 року № 141 (далі – Положення № 141) У розділі II: у пункті 1 слова «і національних стандартів», «, а також нормативних документів з питань розроблення та поставлення продукції на виробництво» виключити; у абзаці двадцятому пункту 10 слова «національними стандартами» замінити словами «нормативно-правовими актами»;	здійснюється відповідно до вимог **нормативно-правових актів** у сферах захисту інформації та інформаційної безпеки, розроблення та поставлення продукції на виробництво»; у пункті 10: у абзаці першому слово «типу» виключити; **абзац двадцятий виключити**;
Пропозиції до пункту 2 Змін (Положення про державну експертизу в сфері криптографічного захисту інформації, затверджене наказом Адміністрації Держспецзв'язку від 23.06.2008 № 100)		
Норма відсутня Витяг з Положення про державну експертизу в сфері криптографічного захисту інформації, затверджене наказом Адміністрації Держспецзв'язку від 23.06.2008 № 100: *«I. Загальні положення* *1.5. Об'єктами експертизи є:* *криптографічні системи, засоби та обладнання КЗІ, **програмно-технічні комплекси центрів сертифікації ключів, надійні засоби електронного цифрового підпису** (далі - криптографічні засоби);»*	**Міністерство економічного розвитку і торгівлі України** Приведення у відповідність до Закону України «Про електронні довірчі послуги» потребує абзац шостий пункту 1.5 розділу I діючого Положення про державну експертизу в сфері криптографічного захисту інформації	1) у розділі I: … у абзаці шостому пункту 1.5 слова «, **програмно-технічні комплекси центрів сертифікації ключів, надійні засоби електронного цифрового підпису**»;

Норма відсутня Витяг з додатку 2 (Перелік документів та матеріалів, необхідних для проведення експертизи криптографічних засобів вітчизняного виробництва) Положення про державну експертизу в сфері криптографічного захисту інформації, затверджене наказом Адміністрації Держспецзв'язку від 23.06.2008 № 100: *«8. Технічна документація на апаратні (апаратно-програмні) компоненти:* *технічні завдання (згідно з ДСТУ 3973-2000 Система розроблення та поставлення продукції на виробництво. Правила виконання науково-дослідних робіт. Загальні положення, ДСТУ 3974-2000 Система розроблення та поставлення продукції на виробництво. Правила виконання дослідно-конструкторських робіт. Загальні положення)* ***та технічні умови (згідно з ДСТУ 1.3:2004 "Національна стандартизація. Правила побудови, викладання, оформлення, погодження, прийняття та позначення технічних умов, ДСТУ - Н 4486:2005 Система конструкторської документації. Настанови щодо типової побудови технічних умов, ГОСТ 2.114-95 "Единая система конструкторской документации. Технические условия")****;* *9. Програмна документація на програмні компоненти:* *технічне завдання* ***(згідно з ГОСТ 19.201-78 "Единая система программной документации. Техническое задание. Требования к содержанию и оформлению")****;*	**Міністерство економічного розвитку і торгівлі України** Пропонуємо внести зміни до діючого Положення про державну експертизу в сфері криптографічного захисту інформації, затвердженому наказом Адміністрації Держспецзв'язку від 23 червня 2008 року № 100: у додатку 2 в абзаці другому пункту 8 слова «та технічні умови (згідно ДСТУ 1.3:2004 «Національна стандартизація. Правила побудови, викладання, оформлення, погодження, прийняття та позначення технічних умов, ДСТУ – Н 4486:2005 Система конструкторської документації. Настанова щодо типової побудови технічних умов, ГОСТ 2.114-95 «Единая система конструкторской документации. Технические условия»)» виключити; у пункті 9: в абзаці другому слова «(згідно з ГОСТ 19.201-78 «Единая система документации. Техническое задание. Требования к содержанию и оформлению»)» виключити (скасовано з	3) у додатку 2: у абзаці другому пункту 8 слова «та технічні умови (згідно ДСТУ 1.3:2004 «Національна стандартизація. Правила побудови, викладання, оформлення, погодження, прийняття та позначення технічних умов, ДСТУ – Н 4486:2005 Система конструкторської документації. Настанова щодо типової побудови технічних умов, ГОСТ 2.114-95 «Единая система конструкторской документации. Технические условия»)» виключити; у пункті 9: у абзаці другому слова «(згідно з ГОСТ 19.201-78 «Единая система документации. Техническое задание. Требования к содержанию и оформлению»)» виключити; у абзаці третьому слова «(згідно з ДСТУ 1.3:2004 Національна стандартизація. Правила побудови, викладання, оформлення, погодження, прийняття та позначення технічних умов (за потреби)» виключити; в абзаці четвертому слова «(згідно з ГОСТ 19.202-78 «Единая система программной документации. Спецификация. Требования к содержанию и оформлению»)» виключити; в абзаці п'ятому слова «(згідно з ГОСТ 19.401-78 «Единая система программной документации. Текст программы. Требования к содержанию и оформлению»)» виключити; в абзаці шостому слова «(згідно з

технічні умови (згідно з ДСТУ 1.3:2004 Національна стандартизація. Правила побудови, викладання, оформлення, погодження, прийняття та позначення технічних умов (за потреби); *специфікація* ***(згідно з ГОСТ 19.202-78 "Единая система программной документации. Спецификация. Требования к содержанию и оформлению")****;* *тексти програм* ***(згідно з ГОСТ 19.401-78 "Единая система программной документации. Текст программы. Требования к содержанию и оформлению")****;* *описи програм* ***(згідно з ГОСТ 19.402-78 "Единая система программной документации. Описание программы")****;* *програма та методика випробувань* ***(згідно з ГОСТ 19.301-79 "Единая система программной документации. Программа и методика испытаний. Требования к содержанию и оформлению");*** *настанова системного програміста* ***(згідно з ГОСТ 19.503-79 "Единая система программной документации. Руководство системного программиста. Требования к содержанию и оформлению")****;* *настанова програміста* ***(згідно з ГОСТ 19.504-79 "Единая система программной документации. Руководство программиста. Требования к содержанию и оформлению")****;*	01.01.2019); абзац третій виключити; в абзаці четвертому слова «(згідно з ГОСТ 19.202-78 «Единая система программной документации. Спецификация. Требования к содержанию и оформлению»)» виключити (скасовано з 01.01.2019); в абзаці п'ятому слова «(згідно з ГОСТ 19.401-78 «Единая система программной документации. Текст программы. Требования к содержанию и оформлению»)» виключити (скасовано з 01.01.2019); в абзаці шостому слова «(згідно з ГОСТ 19.402-78 «Единая система программной документации. Описание программы»)» виключити (скасовано з 01.01.2019); в абзаці сьомому слова «(згідно з ГОСТ 19.301-79 «Единая система программной документации. Программа и методика испытаний. Требования к содержанию и оформлению»)» виключити (скасовано з 01.01.2019); в абзаці восьмому слова «(згідно з ГОСТ 19.503-79 «Единая система программной документации. Руководство системного программиста. Требования к содержанию и оформлению»)» виключити (скасовано з 01.01.2019); в абзаці дев'ятому слова «(згідно з ГОСТ 19.504-79 «Единая система программной документации. Руководство программиста. Требования к содержанию и оформлению»)»	ГОСТ 19.402-78 «Единая система программной документации. Описание программы»)» виключити; в абзаці сьомому слова «(згідно з ГОСТ 19.301-79 «Единая система программной документации. Программа и методика испытаний. Требования к содержанию и оформлению»)» виключити; в абзаці восьмому слова «(згідно з ГОСТ 19.503-79 «Единая система программной документации. Руководство системного программиста. Требования к содержанию и оформлению»)» виключити; в абзаці дев'ятому слова «(згідно з ГОСТ 19.504-79 «Единая система программной документации. Руководство программиста. Требования к содержанию и оформлению»)» виключити; в абзаці десятому слова «(згідно з ГОСТ 19.505-79 «Единая система программной документации. Руководство оператора. Требования к содержанию и оформлению»)» виключити;

настанова оператора ***(згідно з ГОСТ 19.505-79 "Единая система программной документации. Руководство оператора. Требования к содержанию и оформлению").»***	виключити (скасовано з 01.01.2019); в абзаці десятому слова «(згідно з ГОСТ 19.505-79 «Единая система программной документации. Руководство оператора. Требования к содержанию и оформлению»)» виключити (скасовано з 01.01.2019);	
Пропозиції до пункту 4 Змін **(Вимоги до форматів криптографічних повідомлень, затверджені наказом Адміністрації Держспецзв'язку від 18.12.2012 № 739)**		
Норма відсутня Витяг з Вимог до форматів криптографічних повідомлень, затверджені наказом Адміністрації Держспецзв'язку від 18.12.2012 № 739: *«II. Типи повідомлень* *2.2. Тип повідомлення "ContentInfo" подано в нотації ASN.1, яка визначена у ДСТУ ISO/IEC 8824-1:**2009** "Інформаційні технології. Нотація абстрактного синтаксису 1 (ASN.1). Частина 1. Специфікація базової нотації", ДСТУ ISO/IEC 8824-2:**2009** "Інформаційні технології. Нотація абстрактного синтаксису 1 (ASN.1). Частина 2. Специфікація інформаційного об'єкта", ДСТУ ISO/IEC 8824-3:**2009** "Інформаційні технології. Нотація абстрактного синтаксису 1 (ASN.1). Частина 3. Специфікація обмежень", ДСТУ ISO/IEC 8824-4:**2009** "Інформаційні технології. Нотація абстрактного синтаксису 1 (ASN.1). Частина 4. Параметризація специфікацій ASN.1" (далі - ISO/IEC 8824).»*	**Міністерство економічного розвитку і торгівлі України** Внести зміни до діючих Вимог до форматів криптографічних повідомлень: пункт 2.2 розділу II викласти у такій редакції: «2.2 Тип повідомлення «ContentInfo» подано в нотації ASN.1, яка визначена ДСТУ ISO/IEC 8824-1:**2017 (ISO/IEC 8824-1:2015, IDT)** «Інформаційні технології. Нотація абстрактного синтаксису 1 (ASN.1). Частина 1. Специфікація базової нотації», ДСТУ ISO/IEC 8824-2:**2017 (ISO/IEC 8824-2:2015, IDT)** «Інформаційні технології. Нотація абстрактного синтаксису 1 (ASN.1). Частина 2. Специфікація інформаційного об'єкта», **ДСТУ ISO/IEC 8824-3:2008** «Інформаційні технології. Нотація абстрактного синтаксису 1 (ASN.1). Частина 3. Специфікація обмежень», ДСТУ ISO/IEC 8824-4:**2017 (ISO/IEC 8824-4:2015, IDT)** «Інформаційні технології. Нотація абстрактного синтаксису 1 (ASN.1). Частина 4. Параметризація специфікацій ASN.1».	2) у розділі II: пункт 2.2 викласти у такій редакції: «2.2 Тип повідомлення «ContentInfo» подано в нотації ASN.1, яка визначена ДСТУ ISO/IEC 8824-1:2017 (ISO/IEC 8824-1:2015, IDT) «Інформаційні технології. Нотація абстрактного синтаксису 1 (ASN.1). Частина 1. Специфікація базової нотації», ДСТУ ISO/IEC 8824-2:2017 (ISO/IEC 8824-2:2015, IDT) «Інформаційні технології. Нотація абстрактного синтаксису 1 (ASN.1). Частина 2. Специфікація інформаційного об'єкта», ДСТУ ISO/IEC 8824-3:2008 (ISO/IEC 8824-3:2002, IDT) «Інформаційні технології. Нотація абстрактного синтаксису 1 (ASN.1). Частина 3. Специфікація обмежень», ДСТУ ISO/IEC 8824-4:2017 (ISO/IEC 8824-4:2015, IDT) «Інформаційні технології. Нотація абстрактного синтаксису 1 (ASN.1). Частина 4. Параметризація специфікацій ASN.1»;

Пропозиції до пункту 5 Змін (Інструкція про порядок постачання і використання ключів до засобів криптографічного захисту інформації, затверджена наказом Адміністрації Держспецзв'язку від 12.06.2007 року № 114		
Норма відсутня	**Міністерство економічного розвитку і торгівлі України** У тексті діючої Інструкції посилання на ГОСТ 28147-89 який скасовано необхідно виключити.	1) за текстом слова та цифри «ГОСТ 28147-89» замінити словами та цифрами «ДСТУ ГОСТ 28147:2009»;
Норма відсутня *Витяг з Інструкції* **про порядок постачання і використання ключів до засобів криптографічного захисту інформації, затверджена наказом Адміністрації Держспецзв'язку від 12.06.2007 року № 114:** 1.3. Вимоги цієї Інструкції обов`язкові для виконання органами державної влади та органами місцевого самоврядування, підприємствами, установами та організаціями всіх форм власності, які здійснюють розроблення, виробництво, використання, експлуатацію, сертифікаційні випробування, тематичні дослідження, експертизу, увезення, вивезення криптосистем і засобів КЗІ, що реалізують криптографічний алгоритм, визначений ГОСТ 28147-89, надають послуги в галузі КЗІ з використанням зазначених засобів КЗІ (у тому числі **послуги електронного цифрового підпису**), здійснюють їх постачання або торгівлю ними. 1.5. Використані в цій Інструкції терміни мають такі значення: довгостроковий ключовий елемент (далі – ДКЕ) – ключ, що визначає заповнення таблиць	**Міністерство економічного розвитку і торгівлі України** Приведення у відповідність до Закону України «Про електронні довірчі послуги» потребують пункт 1.3, абзац третій, дев'ятий пункту 1.5, пункт 2.4 діючої Інструкції про порядок постачання і використання ключів до засобів криптографічного захисту інформації	2) у главі 1: у пункті 1.1 слова «електронний цифровий підпис» замінити словами «електронні довірчі послуги»; у пункті 1.3 слова «послуги електронного цифрового підпису» замінити словами «електронні довірчі послуги»; у пункті 1.5: у абзаці третьому слова «засобів електронного цифрового підпису» замінити словами «засобів удосконаленого електронного підпису чи печатки, засобів кваліфікованого електронного підпису чи печатки»; у абзаці дев'ятому слова «електронного цифрового підпису» замінити словами «електронних довірчих послуг»; 3) у пункті 2.4 глави 2 слова «посилених» та «електронного цифрового підпису» виключити.

блока підстановки алгоритму криптографічного перетворення, визначеного ГОСТ 28147-89; замовник – юридична особа будь-якої форми власності, яка замовляє встановленим порядком ключі до засобів КЗІ, у тому числі **засобів електронного цифрового підпису**, у яких реалізується криптографічний алгоритм, визначений ГОСТ 28147-89. Як замовники можуть виступати розробники, виробники, постачальники та користувачі засобами КЗІ; … Інші терміни застосовуються у значеннях, наведених у нормативно-правових актах з питань криптографічного захисту інформації, **електронного цифрового підпису**, а також ГОСТ 28147-89. 2.4. У випадках, передбачених пунктом 2.3 цієї Інструкції, ДКЕ можуть також обиратися з **посилених** сертифікатів відкритого ключа **електронного цифрового підпису**.		

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