**ДОДАТОК 4**

*до тендерної документації*

*Примітка: учасник торгів підписує даний документ і скріплює печаткою (за наявності). Учасник не повинен відступати від даної форми документу*

**ПРОЄКТ**

**ДОГОВІР №\_\_\_\_\_\_\_**

**про надання послуг**

м. Київ \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ 2023 року

**Комунальне підприємство «Головний інформаційно-обчислювальний центр»** (надалі – Замовник) в особі в особі \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_, який (яка) діє на підставі \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_, та

**\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_** (надалі – Виконавець) в особі \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_, який (яка) діє на підставі \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_,

надалі Замовник і Виконавець також іменуються Сторона, а спільно Сторони, враховуючи результат проведення закупівлі за ідентифікатором UA-\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_:

**Створення комплексної системи захисту інформації для інформаційно-комунікаційної системи «Програмна платформа для надання електронних послуг, у тому числі адміністративних»**, керуючись Цивільним кодексом України, Господарським кодексом України, пунктом десятим Особливостей здійснення публічних закупівель товарів, робіт і послуг для замовників, передбачених Законом України «Про публічні закупівлі», на період дії правового режиму воєнного стану в Україні та протягом 90 днів з дня його припинення або скасування, затверджених постановою Кабінету Міністрів України від 12 жовтня 2022 р. № 1178, та іншими нормативно-правовими актами України, правом Сторін укладати договори, норми яких не суперечать діючому законодавству, на виконання пункту 16.23 «Створення та проведення державних експертиз КСЗІ автоматизованих систем Київської міської ради, структурних підрозділів виконавчого органу Київської міської ради (Київської міської державної адміністрації), районних в місті Києві державних адміністрацій, підприємств, установ та організацій, що належать до комунальної власності територіальної громади міста Києва» переліку завдань і заходів Комплексної міської цільової програми «Електронна столиця» на 2019-2023 роки, затвердженої рішенням Київської міської ради від 18.12.2018 № 461/6512 (у редакції рішення Київської міської ради від 08.12.2022 № 5824/5865), уклали цей Договір про надання послуг (надалі – Договір) про нижченаведене.

1. **ПРЕДМЕТ ДОГОВОРУ**
   1. Відповідно до пункту 19 Порядку виконання повноважень Державною казначейською службою в особливому режимі в умовах воєнного стану, затвердженого постановою Кабінету Міністрів України № 590 від 09 червня 2021 року, Виконавець зобов’язується надати Замовнику послуги у сфері інформатизації шляхом створення комплексної системи захисту інформації для інформаційно-комунікаційної системи «Програмна платформа для надання електронних послуг, у тому числі адміністративних» з метою досягнення максимальної ефективності захисту за рахунок одночасного цільового використання всіх необхідних ресурсів, методів і засобів, що виключатимуть несанкціонований доступ до інформації, та [створення умов оброблення інформації](http://ndipit.com.ua/ua/poslugy/zahyst-information/neobxidnist-vprovadzhennya) відповідно до вимог чинних нормативно-правових актів України у сфері захисту інформації, а саме: **Виконавець зобов’язується в порядку та на умовах, визначених Договором, надати Замовнику послуги зі створення комплексної системи захисту інформації для інформаційно-комунікаційної системи «Програмна платформа для надання електронних послуг, у тому числі адміністративних»** (далі  – послуги), а Замовник – прийняти і оплатити такі послуги.
   2. Предмет Договору визначено за кодом ДК 021:2015 «Єдиний закупівельний словник» – 72220000-3 Консультаційні послуги з питань систем та з технічних питань.
   3. Обсяги закупівлі послуг можуть бути зменшені Замовником в односторонньому порядку залежно від його фінансового стану та/або його потреб.
   4. Перелік послуг, строки їх надання та вартість визначаються Календарним планом надання послуг, що є Додатком 1 до Договору, який є невід’ємною частиною Договору (далі – Календарний план).
   5. Інформація про необхідні технічні, якісні та кількісні характеристики предмету Договору визначаються в Технічних вимогах (Додатком 2 до Договору, який є невід’ємною частиною Договору, далі – Технічні вимоги).
2. **ЯКІСТЬ ПОСЛУГ ТА ГАРАНТІЙНІ ЗОБОВ’ЯЗАННЯ**
   1. Виконавець повинен надати Замовнику послуги, якість яких відповідає Технічним вимогам й іншим умовам Договору, з урахуванням норм законодавства, державних стандартів і правил та інших встановлених вимог, що зазвичай ставляться до такого виду послуг і діють на території України.
   2. Виконавець забезпечує гарантійну підтримку (супровід) комплексної системи захисту інформації для інформаційно-комунікаційної системи «Програмна платформа для надання електронних послуг, у тому числі адміністративних» (далі – КСЗІ  ІКС), що включає актуалізацію документації КСЗІ ІКС Замовника та надання інформаційно-консультаційної підтримки щодо експлуатації КСЗІ ІКС за запитом Замовника, упродовж строку дії «Атестата відповідності», переданого Виконавцем Замовнику за Актом приймання-передачі наданих послуг по останньому етапу згідно з Календарним планом.
   3. Якщо протягом строку гарантійної підтримки (супроводження) КСЗІ  ІКС виявляються недоліки (дефекти, помилки, неполадки, збої у роботі КСЗІ  ІКС й/або невідповідність наданих послуг Технічним вимогам й іншим умовам Договору, які не могли бути виявлені при прийнятті наданих послуг, Замовник має заявити про них Виконавцю в розумний строк, але не більше ніж протягом 5 (п’яти) робочих днів після ïx виявлення. Не пізніше наступного дня після повідомлення про виявлені недоліки та/або невідповідності Виконавець зобов’язаний прибути до Замовника і Сторони складають акт виявлених недоліків. Виконавець за свій рахунок повинен усунути недоліки та/або невідповідності у терміни, що визначаються у акті виявлених недоліків, але не більше 10 (десяти) робочих днів.
   4. Гарантійне зобов’язання не припиняється у разі неможливості виконання Виконавцем такого зобов’язання. Гарантійний строк продовжується на час, протягом якого КСЗІ  ІКС не могла використовуватись внаслідок недоліків та/або невідповідності наданих послуг, за які відповідає Виконавець.
3. **ЦІНА ДОГОВОРУ ТА ПОРЯДОК РОЗРАХУНКІВ**
   1. Ціна Договору становить: \_\_\_\_\_\_\_\_\_\_\_\_\_\_ грн (\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_), в тому числі ПДВ \_\_\_\_\_\_\_\_\_\_\_\_\_\_ грн (\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_) *(якщо Виконавець – платник ПДВ)*.
   2. Ціна Договору включає в себе всі витрати, пов’язані з наданням послуг, а також зі сплатою всіх можливих податків, зборів та інших обов’язкових платежів, всі інші витрати для виконання Договору. Ціна послуг за кожним етапом надання послуг зазначена в Календарному плані.
   3. Замовник здійснює оплату за Договором поетапно відповідно до Календарного плану з урахуванням такого:

- за рахунок коштів місцевого бюджету Замовник оплачує вартість 1, 2 та 3 етапів послуг у розмірі \_\_\_\_\_\_\_\_\_\_\_\_\_ грн (\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_) протягом 20 (двадцяти) календарних днів з дати підписання Сторонами відповідного акту приймання – передачі наданого етапу послуг;

- за рахунок власних коштів Замовник оплачує вартість 4 етапу послуг у розмірі \_\_\_\_\_\_\_\_\_\_\_\_\_  грн (\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_) протягом 60 (шістдесяти) календарних днів з дати підписання Сторонами відповідного акту приймання – передачі наданого етапу послуг.

* 1. Розрахунки за надані послуги, що здійснюються за рахунок коштів місцевого бюджету, здійснюються відповідно до ст. 49 Бюджетного кодексу України в національній валюті України – гривні, шляхом перерахування Замовником грошових коштів на поточний рахунок Виконавця за фактично надані належної якості послуги й за умови здійснення відповідного бюджетного фінансування на рахунок Замовника.
  2. У випадку відсутності фінансування або його затримки, розрахунки за надані послуги затримуються до моменту надходження фінансування для оплати таких послуг.
  3. Замовник не несе відповідальності за затримку бюджетного фінансування та зобов’язується здійснити оплату вартості наданих Виконавцем послуг протягом 10 робочих днів з дати надходження відповідного бюджетного фінансування на рахунок Замовника.
  4. Ціна Договору може бути змінена у випадках, передбачених Особливостями здійснення публічних закупівель товарів, робіт і послуг для замовників, передбачених Законом України «Про публічні закупівлі», на період дії правового режиму воєнного стану в Україні та протягом 90 днів з дня його припинення або скасування, затвердженими постановою Кабінету Міністрів України від 12 жовтня 2022 р. № 1178.

1. **ПОРЯДОК І СТРОКИ НАДАННЯ ПОСЛУГ**
   1. Місце надання послуг: м. Київ, вул. Космічна, 12 А.
   2. Строк надання послуг: з дати отримання письмової заявки від Замовника і відповідно до Календарного плану. При цьому, у будь-якому випадку послуги за етапами 1, 2, 3 Календарного плану мають бути надані у повному обсязі не пізніше 22 грудня 2023 року, послуги за етапом 4 Календарного плану – не пізніше 31 грудня 2024 року.

Після вказаних дат Замовник має право відмовитись від прийняття послуг в односторонньому порядку шляхом направлення письмового повідомлення про вказане на електронну адресу Виконавця:\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_.

* 1. Виконавець приступає до надання послуг виключно після отримання письмової заявки від Замовника.
  2. Надання послуг здійснюється поетапно згідно з Календарним планом. За рішенням Виконавця, яке попередньо в письмовій формі погоджено Замовником, реалізація етапів може проводитися як послідовно один за одним так і одночасно.
  3. Перелік документації та результати послуг, що підлягають оформленню та здачі Виконавцем Замовнику, визначаються Календарним планом.
  4. Приймання наданих послуг здійснюється Замовником з урахуванням їх відповідності вимогам Договору, в тому числі Календарному плану та Технічним вимогам.
  5. По завершенню кожного з етапів Договору Виконавець надає Замовнику Акт приймання-передачі наданих послуг за відповідним етапом з доданням результату відповідного етапу послуг згідно з Календарним планом.
  6. Приймання та оцінка наданих послуг за відповідним етапом здійснюється впродовж 5 (п’яти) робочих днів з дати надання Виконавцем Замовнику Акту приймання-передачі наданих послуг комісією Замовника. Робота комісії завершується складанням відповідного протоколу з висновком про відповідність наданих послуг умовам Договору та підписанням Замовником Акту приймання-передачі наданих послуг. У разі виявлення комісією Замовника невідповідностей наданих послуг вимогам Договору комісією складається протокол з висновком про невідповідність наданих послуг умовам Договору із зазначенням переліку необхідних доопрацювань і строками їх виконання.
  7. Виконавець зобов’язаний, без додаткової оплати, впродовж 10 (десяти) календарних днів або в інший узгоджений із Замовником строк, вжити всіх заходів й усунути недоліки наданих послуг відповідно до протоколу з висновком про невідповідність наданих послуг.
  8. Після усунення недоліків наданих послуг, повторні приймання та оцінка наданих Виконавцем послуг здійснюється в порядку, визначеному цим розділом Договору.

1. **ПРАВА ТА ОБОВ’ЯЗКИ СТОРІН**
   1. *Замовник зобов’язаний:*
      1. Своєчасно та в повному обсязі сплачувати вартість належним чином наданих послуг з урахуванням п.п. 3.4.-3.6. Договору.
      2. Приймати надані послуги за відповідним етапом згідно з умовами Договору, в тому числі Календарним планом, за Актами приймання-передачі наданих послуг за відповідним етапом.
      3. На письмову вимогу Виконавця надавати йому інформацію, необхідну для надання послуг за Договором.
      4. Призначити особу, відповідальну за взаємодію з фахівцями Виконавця для надання Виконавцем послуг за Договором.
      5. При виявлені недоліків (невідповідностей) наданих послуг, невідкладно інформувати про це Виконавця.
      6. При встановлені недоліків та/або невідповідностей наданих послуг, повідомляти про це Виконавця.
   2. *Замовник має право:*
      1. Вимагати від Виконавця надання послуг за відповідним етапом у строки, встановлені Договором, в тому числі Календарним планом.
      2. Контролювати якість та строки надання послуг за Договором.
      3. Зменшувати в односторонньому порядку обсяг закупівлі послуг та, відповідно ціну Договору, залежно від реального фінансового стану та/або потреб.
      4. Повернути Виконавцю Акти приймання-передачі наданих послуг без здійснення оплати в разі неналежного оформлення або не оформлення документів, передбачених Договором.
      5. Вимагати від Виконавця надання послуг, якість яких відповідає умовам, встановленим Договором.
      6. Відмовитись від приймання послуг, якщо вони не відповідають умовам Договору.
      7. Вимагати від Виконавця безоплатного виправлення недоліків та/або невідповідностей, що виникли внаслідок допущених Виконавцем порушень Договору, зокрема виконання гарантійних зобов’язань протягом гарантійного строку, зазначеного у п. 2.2. Договору.
      8. Відмовитись від своїх зобов’язань за Договором та розірвати Договір в односторонньому порядку, повідомивши про це Виконавця, у разі:

* якщо Виконавець не розпочав надання послуг у встановлені строки або порушує строки надання послуг;
* якщо Виконавець не усуне недоліки та/або невідповідності наданих послуг відповідно до умов Договору;
* якщо Сторони не дійдуть згоди щодо зміни істотних умов Договору у випадках, передбачених Особливостями здійснення публічних закупівель товарів, робіт і послуг для замовників, передбачених Законом України «Про публічні закупівлі», на період дії правового режиму воєнного стану в Україні та протягом 90 днів з дня його припинення або скасування, затвердженими постановою Кабінету Міністрів України від 12 жовтня 2022 р. № 1178.
  + 1. Вимагати від Виконавця відшкодування збитків, якщо вони виникли внаслідок невиконання або неналежного виконання Виконавцем взятих на себе зобов’язань за Договором.
    2. Застосування Замовником п.5.2.8. Договору не звільняє Виконавця від відповідальності за невиконання/неналежне виконання зобов’язань за Договором та від відшкодування Замовнику пов’язаних із цим збитків.
  1. *Виконавець зобов’язаний:*
     1. Надати Замовнику послуги за відповідним етапом у строки, встановлені Договором, в тому числі Календарним планом.
     2. Забезпечити надання послуг, якість та комплектність яких відповідає умовам, встановленим Договором, в тому числі Технічним вимогам.
     3. Дотримуватись робочого розпорядку, що діє у Замовника, правил охорони праці та пожежної безпеки під час перебування на території Замовника.
     4. За свій рахунок виконувати гарантійні зобов’язання протягом гарантійного строку на умовах, встановлених Договором.
     5. Не брати участь у легалізації («відмиванні») доходів, одержаних злочинним шляхом, а саме не вчиняти будь-які дії, пов’язані із вчиненням фінансової операції чи правочину з активами, одержаними внаслідок вчинення злочину, а також вчиненням дій, спрямованих на приховання чи маскування незаконного походження таких активів або володіння ними, прав на такі активи, джерел їх походження, місцезнаходження, переміщення, зміну їх форми (перетворення), а також набуттям, володінням або використанням активів, одержаних внаслідок вчинення злочину.
     6. Виконувати інші обов’язки, передбачені Договором та законодавством України.
  2. *Виконавець має право:*
     1. Своєчасно та в повному обсязі отримувати плату за надані послуги в порядку, визначеному Договором.
     2. Вимагати відшкодування збитків і сплати штрафних санкцій за порушення Замовником умов Договору.
     3. Відмовитись від своїх зобов’язань за Договором та розірвати Договір в односторонньому порядку, повідомивши про це Замовника, у разі якщо Сторони не дійдуть згоди щодо зміни істотних умов Договору у випадках, передбачених чинним законодавством.

1. **ВІДПОВІДАЛЬНІСТЬ СТОРІН**
   1. У разі невиконання або неналежного виконання своїх зобов’язань за Договором, Сторони несуть відповідальність, передбачену чинним законодавством України та Договором.
   2. За порушення строків виконання зобов’язань за Договором Виконавець сплачує Замовнику пеню у розмірі подвійної облікової ставки НБУ від вартості послуг, з яких допущено прострочення, за кожний день прострочення.

За невиконання гарантійних зобов’язань, в тому числі порушення строків їх виконання, Виконавець сплачує Замовнику штраф в розмірі 5 000,00 грн за кожний випадок невиконання/порушення строків виконання.

* 1. У разі якщо прострочення встановлених строків надання послуг за етапом перевищує 10 (десять) календарних днів Виконавець додатково сплачує Замовнику штраф у розмірі 10 % (десяти відсотків) від вартості послуг, з яких допущено прострочення. Сплата пені, штрафу може за рішенням Замовника відбувається шляхом утримання Замовником грошових коштів з суми коштів, що належить до перерахування Виконавцю відповідно до п.3.3. Договору.
  2. У разі невиконання або неналежного виконання Виконавцем зобов’язань щодо якості наданих послуг та/або надання послуг, що не відповідають Технічним вимогам, Виконавець сплачує штраф у розмірі 20% (двадцяти відсотків) від вартості неякісно наданих послуг, а Замовник має право відмови від оплати за неякісно надані та/або надані з порушенням Технічних вимог послуги із звільненням Замовника від будь-якої відповідальності за такі дії.
  3. Збитки, завдані Замовнику неналежним виконанням Виконавцем зобов’язань за Договором, підлягають відшкодуванню у повній сумі понад встановлені Договором штрафні санкції.
  4. Якщо Виконавець є платником ПДВ, Виконавець зобов’язується зареєструвати податкову накладну в Єдиному реєстрі податкових накладних в строки відповідно до чинного законодавства України.

У разі не виконання або несвоєчасного виконання Виконавцем вимог законодавства щодо складання податкової накладної та/або реєстрації її в Єдиному реєстрі податкових накладних, внаслідок чого Замовник втратив право на включення суми податку на додану вартість до податкового кредиту за відповідний звітний період, Виконавець відшкодовує Замовнику зазначену суму податку на додану вартість. Відшкодування здійснюється на підставі вимоги Замовника у семиденний строк від дня пред’явлення вимоги. Вимога може бути пред’явлена протягом трьох років з моменту втрати Замовником права на включення суми податку на додану вартість до податкового кредиту за відповідний звітний період.

* 1. У разі порушення встановленого умовами Договору строку виконання зобов’язань з оплати крім випадків, зазначених в п.п. 3.4.-3.6. Договору, Замовник сплачує Виконавцю пеню у розмірі подвійної облікової ставки НБУ від суми заборгованості, за кожний день прострочення.
  2. Сторони за порушення господарських зобов’язань за Договором можуть застосовувати такі оперативно-господарські санкції:

1) одностороння відмова від виконання свого зобов’язання управленою Стороною із звільненням її від відповідальності за це – у разі порушення зобов’язання другою Стороною;

2) відмова від встановлення на майбутнє господарських відносин із Стороною, яка порушує зобов’язання.

1. **ОБСТАВИНИ НЕПЕРЕБОРНОЇ СИЛИ**
   1. Сторони звільняються від відповідальності за невиконання або неналежне виконання зобов’язань за Договором у разі виникнення обставин непереборної сили, які не існували під час укладення Договору та виникли поза волею Сторін. Форс-мажорними обставинами (обставинами непереборної сили) є надзвичайні та невідворотні обставини, що об’єктивно унеможливлюють виконання зобов’язань, передбачених умовами Договору, загроза війни, збройний конфлікт або серйозна погроза такого конфлікту, включаючи, але не обмежуючись ворожими атаками, блокадами, військовим ембарго, дії іноземного ворога, загальна військова мобілізація, військові дії, оголошена та неоголошена війна, дії суспільного ворога, збурення, акти тероризму, диверсії, піратства, безлади, вторгнення, блокада, революція, заколот, повстання, масові заворушення, введення комендантської години, експропріація, примусове вилучення, захоплення підприємств, реквізиція, громадська демонстрація, блокада, страйк, аварія, протиправні дії третіх осіб, пожежа, вибух, тривалі перерви в роботі транспорту, регламентовані умовами відповідних рішень та актами державних органів влади, а також викликані винятковими погодними умовами і стихійним лихом, а саме: епідемія, сильний шторм, циклон, ураган, торнадо, буревій, повінь, нагромадження снігу, ожеледь, град, заморозки, землетрус, блискавка, пожежа, посуха, просідання і зсув ґрунту, інші стихійні лиха тощо; перебої в електроживленні, глобальні перебої в роботі українських і міжнародних сегментів мережі Інтернет, збої систем маршрутизації, збої в розподіленій системі доменних імен, збої, викликані хакерськими і DDOS-атаками тощо.
   2. Сторона, що не може виконувати зобов’язання за Договором унаслідок дії обставин непереборної сили, повинна не пізніше ніж протягом 5 (п’яти) календарних днів з моменту їх виникнення повідомити про це іншу Сторону у письмовій формі та надати підтверджуючі документи. Несвоєчасне повідомлення про існування обставин форс-мажору та надання підтверджуючих документів позбавляє відповідну Сторону права посилатися на них як на обставини, що звільняють від відповідальності за повне або часткове невиконання зобов’язання.
   3. Доказом виникнення обставин непереборної сили та строку їх дії є відповідні документи, які видаються Торгово-промисловою палатою України, провайдерами електронних комунікацій або іншим компетентним органом.
   4. У разі існування обставин, передбачених п.7.1. Договору (за умови дотримання вимог п.7.2. Договору), строк надання послуг та дія Договору продовжуються на час існування таких обставин.

У разі коли строк дії обставин непереборної сили продовжується більше ніж 30 (тридцять) днів, кожна із Сторін в установленому порядку має право розірвати цей Договір.

1. **ВИРІШЕННЯ СПОРІВ**
   1. У випадку виникнення спорів або розбіжностей Сторони зобов’язуються вирішувати їх шляхом взаємних переговорів та консультацій.
   2. У разі недосягнення Сторонами згоди, спори (розбіжності) вирішуються у судовому порядку, згідно правил підвідомчості і підсудності, встановлених чинним законодавством України.
2. **СТРОК ДІЇ ДОГОВОРУ**
   1. Договір набирає чинності з дати його підписання і діє до 31 грудня 2024 року, а в частині розрахунків та гарантійних зобов’язань за Договором – до повного виконання їх Сторонами.
   2. Закінчення строку дії Договору не звільняє Сторони від відповідальності за його порушення, що мало місце під час дії Договору.
3. **АНТИКОРУПЦІЙНІ ПОЛОЖЕННЯ ТА ЗАСТЕРЕЖЕННЯ**
   1. Сторони повністю дотримуються принципів протидії усім формам корупції, забезпечують регулярну оцінку корупційних ризиків в своїй діяльності і здійснюють антикорупційні заходи.
   2. Усім працівникам Сторін заборонено приймати або пропонувати прямо чи опосередковано в процесі виконання ними своїх обов’язків гроші, подарунки, послуги, будь-які інші матеріальні винагороди з метою спонукання здійснити або не здійснювати певні дії залежно від можливостей їхньої роботи чи посади.
   3. Сторони зобов’язуються інформувати одна одну про будь-який конфлікт інтересів, факти корупції, що можуть вплинути на виконання Договору.
4. **ІНШІ УМОВИ**
   1. Істотні умови Договору не можуть змінюватися після його підписання до виконання зобов’язань Сторонами в повному обсязі, крім випадків, передбачених Особливостями здійснення публічних закупівель товарів, робіт і послуг для замовників, передбачених Законом України «Про публічні закупівлі», на період дії правового режиму воєнного стану в Україні та протягом 90 днів з дня його припинення або скасування, затвердженими постановою Кабінету Міністрів України від 12 жовтня 2022 р. № 1178.
   2. Сторони вживають всіх заходів для того, щоб їхні співробітники не розголошували інформацію, яка вважається конфіденційною за Договором, без попередньої згоди на це другої Сторони.
   3. Жодна із Сторін не має права передавати свої права та обов’язки за Договором третім особам без письмової згоди на те іншої Сторони.
   4. Всі письмові повідомлення, передбачені Договором, направляються за адресами, вказаними в Договорі, рекомендованою поштою з повідомленням про вручення, або вручаються представникам Сторін особисто під розпис. У разі, якщо повідомлення не буде отримано Стороною, що буде підтверджено поверненням поштового повідомлення з відміткою про неможливість вручення, в тому числі на підставі зміни стороною-одержувачем адреси, вказаної в Договорі, про що інша Сторона не була сповіщена, повідомлення вважатиметься отриманим з дати його відправлення незалежно від фактичного отримання.
   5. Підписуючи Договір, уповноважені представники Сторін дають згоду (дозвіл) на обробку їх персональних даних. Представники Сторін підписанням цього Договору підтверджують, що вони повідомлені про свої права відповідно до ст. 8 Закону України «Про захист персональних даних».
   6. Підписуючи Договір, уповноважені представники Сторін дають згоду (дозвіл) щодо можливості оприлюднення інформації, зазначеної у Договорі та документах, які підтверджують його виконання (Договір, акт приймання-передачі наданих послуг тощо).
   7. Договір складений при повному розумінні Сторонами його умов та термінології, українською мовою у двох автентичних примірниках, які мають однакову юридичну силу – по одному для кожної із Сторін.
   8. Умови Договору можуть бути змінені за згодою Сторін у порядку, визначеному законодавством України, шляхом укладення Сторонами додаткової угоди до Договору. Всі зміни та доповнення до Договору будуть мати юридичну силу, якщо вони виконані в письмовій формі та належним чином підписані уповноваженими представниками Сторін. Такі зміни та доповнення до Договору вважаються його невід’ємною частиною.
   9. Всі виправлення за текстом Договору мають юридичну силу та можуть враховуватися виключно за умови, що вони у кожному окремому випадку датовані та засвідчені підписами Сторін.
   10. Про зміни реквізитів, установчих документів, організаційно-правової форми тощо Сторони у письмовій формі зобов’язані протягом 7 (семи) робочих днів повідомити одна одну.
   11. Виконавець є платником \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_.
   12. Замовник є платником податку на прибуток підприємств на загальних підставах.
5. **ЗАХИСТ ІНФОРМАЦІЇ**
   1. Сторони зобов’язується не розголошувати та не розкривати інформацію (далі за текстом  – «Інформація») третім особам та не використовувати її в будь-яких цілях інакше, ніж в цілях належного виконання Договору, як протягом строку його дії, так і після його припинення.

Під Інформацією розуміється, інформація яка:

- зберігається в письмовій, електронній або в будь-якій іншій матеріальній формі й стосується будь-яких персональних даних фізичних осіб;

- є інформацією про відповідні засоби авторизації (логін, пароль), які дозволяють ідентифікувати представників Сторін в комп’ютерних програмах (інформаційних, інформаційно-комунікаційних системах тощо);

- надана для виконання Договору або стала відома під час виконання Договору.

* 1. Сторони погоджуються з тим, що будь-яка Інформація, яка передається в усній формі, буде вважатися Інформацією до того часу, як неконфіденційний характер такої інформації буде підтверджений в письмовій формі.
  2. Будь-яка Інформація буде передаватися Сторонами виключно для обмеженого використання з метою виконання Договору.
  3. Сторона, якій адресована Інформація (далі за текстом цього розділу – «Отримувач»), зобов’язується:
     1. Зберігати Інформацію, розкритої Стороною, що її розкриває (далі за текстом цього розділу  – «Надавач»).
     2. Не використовувати Інформацію без попередньої письмової згоди Надавача.
     3. Надавати доступ до Інформації тільки тим працівникам, яким необхідно знати таку Інформацію для виконання своїх службових обов’язків, Договору. При цьому Отримувач повинен забезпечити дотримання вказаними працівниками зобов’язань щодо збереження інформації, передбачених Договором, й несе відповідальність за дотримання вказаними працівниками зобов’язань щодо захисту інформації, передбачених Договором.
  4. Кожна Сторона цим визнає, що несанкціоноване розкриття або використання Інформації іншої Сторони може заподіяти непоправну шкоду іншій Стороні.
  5. Інформація, отримана від Надавача, не буде вважатися Інформацією з обмеженим доступом у випадку:

- Інформація була доступна широкому колу осіб на момент її розкриття Отримувачу;

- Інформація після отримання від Надавача стала доступною широкому колу осіб з джерел, не пов’язаних із Отримувачем;

- Надавач в письмовій формі надав згоду на розкриття Інформації.

* 1. Сторони погоджуються, що Отримувач може надати інформацію третім особам в прямо передбачених чинним законодавством України випадках, які зобов’язують Отримувача поширити таку інформацію на вимогу третіх осіб (рішення суду, офіційний запит правоохоронних або інших компетентних державних органів).
  2. Зобов’язання, що містяться в цьому Розділі, є чинними впродовж 5 (п’яти) років з моменту одержання конкретної Інформації, незалежно від припинення дії Договору. Виключенням з цього правила є випадки, коли Надавачем встановлено іншу тривалість дії заборони на розголошення, про що Надавач в письмовій формі повідомив Отримувача.
  3. Припинення дії Договору не припиняє зобов’язань Сторін щодо нерозголошення Інформації, яка була розкрита в період його дії.
  4. Сторони несуть відповідальність за безпідставне поширення Інформації відповідно до чинного законодавства України. Сторона, що допустила безпідставне поширення Інформації, зобов’язується відшкодувати іншій Стороні збитки, спричинені таким поширенням, а також компенсувати упущену вигоду.

1. **ІНШІ ЗОБОВʼЯЗАННЯ ВИКОНАВЦЯ**
   1. Виконавець підтверджує та гарантує, що на момент укладення Договору та протягом всього строку його дії:

(а) він не є резидентом та/чи громадянином російської федерації/республіки білорусь/ держави-агресора (крім передбачених законодавством виключень), та не є суб’єктом господарювання/юридичною особою, створеним/створеною та/або зареєстрованим/ зареєстрованою відповідно до законодавства російської федерації/республіки білорусь/держави-агресора;

(б) російська федерація/республіка білорусь/держава-агресор, громадяни російської федерації/республіки білорусь/держави-агресора (крім передбачених законодавством виключень), або юридична особа, створена та зареєстрована відповідно до законодавства російської федерації/республіки білорусь/держави-агресора, не є кінцевими бенефіціарними власниками (власником) Виконавця та/або членом та/або учасником (акціонером), що має частку в статутному капіталі Виконавця 10 і більше відсотків;

(в) Виконавець не здійснює продаж товарів, робіт, послуг походженням з російської федерації/республіки білорусь/держави-агресора, у тому числі і ті, що є предметом цього Договору;

(г) до Виконавця не застосовано персональні спеціальні економічні та інші обмежувальні заходи (санкції) відповідно до законодавства та/або міжнародних договорів.

* 1. Виконавець зобов’язується:

(а) у разі зміни інформації щодо будь-якої із зазначених вище гарантій протягом 3 (трьох) робочих днів від дати зміни в статусі інформації письмово проінформувати про це Замовника;

(б) не залучати третіх осіб, які не відповідають характеристикам, наведеним у п.п. (а)-(г) п. 13.1, до виконання зобов’язань за цим Договором.

* 1. Замовник має право на розірвання Договору в односторонньому порядку шляхом письмового повідомлення Виконавця не пізніше ніж за 5 (п’ять) робочих днів до дати такого розірвання у разі:

(а) виявлення Замовником обставин, що свідчать про порушення Виконавцем гарантій та зобов’язань, наданих у п. 13.1 та п.п.(б) п. 13.2 Договору;

(б) отримання від Виконавця повідомлення, зазначеного у п.п.(а) п. 13.2 Договору.

1. **ДОДАТКИ ДО ДОГОВОРУ**
   1. Невід’ємними частинами Договору є:
      1. Додаток 1 – Календарний план надання послуг.
      2. Додаток 2 – Технічні вимоги.
   2. Усі додатки до Договору є обов’язковими для виконання Сторонами, якщо вони підписані уповноваженими представниками обох Сторін, скріплені печатками Сторін, мають порядковий номер, а також посилання на дату та номер Договору.
2. **РЕКВІЗИТИ СТОРІН**

|  |  |
| --- | --- |
| **ЗАМОВНИК** | **ВИКОНАВЕЦЬ** |
| **Комунальне підприємство «Головний інформаційно-обчислювальний центр»** |  |
| **\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_**  **м. п.** | **\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_**  **м. п.** |

Додаток 1

до Договору №\_\_\_\_\_\_

про надання послуг

від \_\_\_\_\_\_\_\_\_\_\_\_2023 року

**КАЛЕНДАРНИЙ ПЛАН НАДАННЯ ПОСЛУГ**

**зі створення комплексної системи захисту інформації для інформаційно-комунікаційної системи**

**«Програмна платформа для надання електронних послуг, у тому числі адміністративних»**

| **№ з/п** | **Назва етапу** | **Строк виконання\*** | **Документація, що надається за етапом** | **Вартість послуг без ПДВ, грн.** | **ПДВ, грн.** | **Вартість послуг з ПДВ, грн.** |
| --- | --- | --- | --- | --- | --- | --- |
| 1  11 | Підготовка загальних вимог до комплексної системи захисту інформації для інформаційно-комунікаційної системи «Програмна платформа для надання електронних послуг, у тому числі адміністративних», розроблення та оформлення політик безпеки інформації, здійснення вибору основних рішень з протидії всім суттєвим загрозам, обстеження середовища функціонування інформаційно-комунікаційної системи «Програмна платформа для надання електронних послуг, у тому числі адміністративних», розроблення пропозицій щодо забезпечення можливості розвитку/модернізації захищених систем, розроблення Технічного завдання та узгодження Технічного завдання з Державною службою спеціального зв’язку та захисту інформації України. | 15 календарних днів з дати отримання письмової заявки від Замовника | Документація:  1. Проєкт «Положення про службу захисту інформації».  2. Проєкти посадових інструкцій фахівців служби захисту інформації.  3. Проєкт наказу Комунального підприємства «Головний інформаційно-обчислювальний центр» про створення служби захисту інформації.  4. Акт обстеження середовищ функціонування інформаційно-комунікаційної системи «Програмна платформа для надання електронних послуг, у тому числі адміністративних».  5. «Пропозиції щодо порядку проведення експертних досліджень та формування експертних висновків в ІКС ГІОЦ з урахуванням розвитку інформаційних систем КП ГІОЦ, їх модернізації та вдосконалення. Звіт за результатами обстеження інформаційної інфраструктури КП ГІОЦ».  6. «Пропозиції щодо внесення вимог нормативних документів з питань захисту інформації до технічних завдань з розроблення програмного забезпечення ІКС КП ГІОЦ з метою посилення заходів безпеки під час розроблення».  7. Звіт за результатами ознайомлення з документацією на інформаційно-комунікаційну систему «Програмна платформа для надання електронних послуг, у тому числі адміністративних».  8. «Технічне завдання на створення комплексної системи захисту інформації для інформаційно-комунікаційної системи «Програмна платформа для надання електронних послуг, у тому числі адміністративних».  9. «Модель загроз інформації. Модель порушника»;  10. «Політика безпеки інформації в ІКС «Програмна платформа для надання електронних послуг, у тому числі адміністративних». |  |  |  |
| 22 | Розроблення проєкту комплексної системи захисту інформації для інформаційно-комунікаційної системи «Програмна платформа для надання електронних послуг, у тому числі адміністративних» | 10 календарних днів з дати отримання письмової заявки від Замовника | Документація техноробочого проекту на створення комплексної системи захисту інформації для інформаційно-комунікаційної системи «Програмна платформа для надання електронних послуг, у тому числі адміністративних» у складі:   1. Інструкцій з експлуатації комплексної системи захисту інформації для інформаційно-комунікаційної системи «Програмна платформа для надання електронних послуг, у тому числі адміністративних» та її елементів. 2. Процедур регламентного обслуговування комплексної системи захисту інформації для інформаційно-комунікаційної системи «Програмна платформа для надання електронних послуг, у тому числі адміністративних». 3. Правил і положення проведення випробувань і аналізу роботи комплексної системи захисту інформації для інформаційно-комунікаційної системи «Програмна платформа для надання електронних послуг, у тому числі адміністративних». 4. Керівництва адміністраторів комплексної системи захисту інформації для інформаційно-комунікаційної системи «Програмна платформа для надання електронних послуг, у тому числі адміністративних»   і користувачів комплексної системи захисту інформації для інформаційно-комунікаційної системи «Програмна платформа для надання електронних послуг, у тому числі адміністративних». |  |  |  |
| 33 | Введення комплексної системи захисту інформації для інформаційно-комунікаційної системи «Програмна платформа для надання електронних послуг, у тому числі адміністративних» у дію та оцінювання захищеності інформації в інформаційно-комунікаційній системі «Програмна платформа для надання електронних послуг, у тому числі адміністративних» | 5 календарних днів з дати отримання письмової заявки від Замовника | Документація:  1. Програма та методика проведення випробувань.  2. Протокол проведення попередніх випробувань.  3. Проєкт акту про прийняття в дослідну експлуатацію.  4. Проєкт акту завершення дослідної експлуатації.  5. Проєкт акту завершення робіт зі створення комплексної системи захисту інформації в інформаційно-комунікаційній системі «Програмна платформа для надання електронних послуг, у тому числі адміністративних».  6. Звіт про проведення навчання користувачів та комплектування комплексної системи захисту інформації.  7. Проєкт заявки на проведення державної експертизи комплексної системи захисту інформації. |  |  |  |
| 44 | Супровід проведення державної експертизи комплексної системи захисту інформації для інформаційно-комунікаційної системи «Програмна платформа для надання електронних послуг, у тому числі адміністративних» та отримання «Атестата відповідності» | 60 календарних днів з дати отримання письмової заявки від Замовника | Документація:  1. Програма проведення державної експертизи комплексної системи захисту інформації для інформаційно-комунікаційної системи «Програмна платформа для надання електронних послуг, у тому числі адміністративних».  2. Методика проведення державної експертизи комплексної системи захисту інформації для інформаційно-комунікаційної системи «Програмна платформа для надання електронних послуг, у тому числі адміністративних».  3. Атестат відповідності.  4. Експертний висновок, який додається до Атестата відповідності. |  |  |  |

*\* Виконавець має право дострокової здачі етапів*

|  |  |
| --- | --- |
| **ЗАМОВНИК** | **ВИКОНАВЕЦЬ** |
| **Комунальне підприємство «Головний інформаційно-обчислювальний центр»** |  |
| **\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_**  **м. п.** | **\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_**  **м. п.** |

Додаток 2

до Договору №\_\_\_\_\_\_

про надання послуг

від \_\_\_\_\_\_\_\_\_\_\_\_2023 року

**ТЕХНІЧНІ ВИМОГИ**

**ІНФОРМАЦІЯ ПРО НЕОБХІДНІ ТЕХНІЧНІ, ЯКІСНІ ТА КІЛЬКІСНІ ХАРАКТЕРИСТИКИ ПРЕДМЕТА ЗАКУПІВЛІ**

**Надання послуг зі створення комплексної системи захисту інформації для інформаційно-комунікаційної системи «Програмна платформа для надання електронних послуг, у тому числі адміністративних»**

Створення комплексної системи захисту інформації для інформаційно-комунікаційної системи **«**Програмна платформа для надання електронних послуг, у тому числі адміністративних**»** з проведенням державної експертизи цієї комплексної системи захисту інформації здійснюється на виконання пункту 16.23 «Створення та проведення державних експертиз КСЗІ автоматизованих систем Київської міської ради, структурних підрозділів виконавчого органу Київської міської ради (Київської міської державної адміністрації), районних в місті Києві державних адміністрацій, підприємств, установ та організацій, що належать до комунальної власності територіальної громади міста Києва» переліку завдань і заходів Комплексної міської цільової програми «Електронна столиця» на 2019-2023 роки, затвердженої рішенням Київської міської ради від 18.12.2018 № 461/6512 (у редакції рішення Київської міської ради від 08.12.2022 № 5824/5865), та відповідно до вимог законів України «Про інформацію», «Про доступ до публічної інформації», «Про захист інформації в інформаційно-комунікаційних системах», «Про захист персональних даних» та інших нормативно-правових актів України у сфері інформаційної безпеки.

Державна експертиза у сфері технічного захисту інформації комплексних систем захисту інформації інформаційно-телекомунікаційних систем повинна проводитися у відповідності до вимог «Положення про державну експертизу в сфері технічного захисту інформації», затвердженого наказом Адміністрації Державної служби спеціального зв’язку та захисту інформації України від 16.05.2007 № 93, що зареєстроване в Міністерстві юстиції України 16.07.2007 за № 820/14087, та НД ТЗІ 2.6-001-2011 Порядок проведення робіт з державної експертизи засобів технічного захисту інформації від несанкціонованого доступу та комплексних систем захисту інформації в інформаційно-телекомунікаційних системах, затвердженого наказом Адміністрації Державної служби спеціального зв’язку та захисту інформації України від 25.03.2011 № 65.

ПЕРЕЛІК УМОВНИХ СКОРОЧЕНЬ, ОСНОВНИХ ТЕРМІНІВ ТА ВИЗНАЧЕНЬ

| **Терміни та скорочення** | **Визначення** |
| --- | --- |
| Адміністратор | Комунальне підприємство «Головний інформаційно-обчислювальний центр» (КП ГІОЦ) |
| Виконавець | Виконавець послуг зі створення КСЗІ ІКС |
| ДССЗЗІ | Державна служба спеціального зв’язку та захисту інформації України |
| ДСТУ | Державний стандарт України |
| Замовник | Комунальне підприємство «Головний інформаційно-обчислювальний центр» (КП ГІОЦ) |
| ІКС | Інформаційно-комунікаційна система, інформаційна система, автоматизована система, а також інформаційно-телекомунікаційна система, якщо така система була створена, придбана або отримана до набрання чинності Закону України «Про електронні комунікації» та не перейменована. Інформаційно-комунікаційна система складається з компонентів апаратного забезпечення, компонентів програмного забезпечення (системне ПЗ, прикладне ПЗ), компонентів, що забезпечують мережну взаємодію та персоналу, який забезпечує функціонування вищезазначених компонентів |
| ІКС «Програмна платформа для надання електронних послуг, у тому числі адміністративних» | Інформаційно-комунікаційна система «Програмна платформа для надання електронних послуг, у тому числі адміністративних», що створена для реалізації права кожного на доступ до електронних послуг та інших послуг, звернення до Київської міської ради, виконавчого органу Київської міської ради (Київської міської державної адміністрації) та його структурних підрозділів, районних в місті Києві державних адміністрацій та їх структурних підрозділів, підприємств, установ і організацій, що належать до комунальної власності територіальної громади міста Києва або координація діяльності яких здійснюється виконавчим органом Київської міської ради (Київської міської державної адміністрації) з питань отримання таких послуг, отримання інформації з електронних інформаційних ресурсів, інших інформаційно-комунікаційних систем територіальної громади міста Києва, яка необхідна для надання електронних послуг, у тому числі в автоматичному режимі, а також для проведення моніторингу та оцінки якості послуг в установленому порядку |
| КЗЗ | Комплекс засобів захисту (сукупність програмно-апаратних засобів, які забезпечують реалізацію політики безпеки інформації) |
| КСЗІ | Комплексна система захисту інформації |
| НД | Нормативний документ |
| НД ТЗІ | Нормативний документ системи технічного захисту інформації Державної служби спеціального зв’язку та захисту інформації України |
| СЗІ | Служба захисту інформації |
| ТЗ | Технічне завдання на створення комплексної системи захисту інформації для інформаційно-комунікаційної системи **«**Програмна платформа для надання електронних послуг, у тому числі адміністративних» |
| ТЗІ | Технічний захист інформації |

# ЗАГАЛЬНІ ВІДОМОСТІ

## Загальні положення

В цьому документі наведені технічні та якісні характеристики, перелік і терміни надання послуг зі створення комплексної системи захисту інформації для інформаційно-комунікаційної системи «Програмна платформа для надання електронних послуг, у тому числі адміністративних» з проведенням державної експертизи комплексної системи захисту інформації (далі  КСЗІ ІКС).

## Склад послуг зі створення КСЗІ ІКС

Процес створення КСЗІ ІКС має бути побудований відповідно до вимог законодавства України, вимог національних стандартів України та чинних нормативних документів системи технічного захисту інформації Державної служби спеціального зв’язку та захисту інформації України (далі – НД ТЗІ).

В ході надання послуг з побудови комплексної системи захисту інформації в разі необхідності доопрацювання наявної в Замовника документації на ІКС «Програмна платформа для надання електронних послуг, у тому числі адміністративних» або розширення її комплектності Виконавець має надати проєкти відповідних документів. Нижче наведено перелік послуг зі створення КСЗІ ІКС.

У межах надання послуг зі створення КСЗІ ІКС повинні бути здійснені такі заходи:

1. Підготовка загальних вимог до КСЗІ ІКС.
2. Розроблення та оформлення політик безпеки інформації в ІКС «Програмна платформа для надання електронних послуг, у тому числі адміністративних», здійснення вибору основних рішень з протидії всім суттєвим загрозам.
3. Розроблення пропозицій щодо забезпечення можливості розвитку/модернізації захищених систем.
4. Розроблення ТЗ.
5. Розроблення проєкту КСЗІ ІКС.
6. Введення КСЗІ ІКС у дію та оцінювання захищеності інформації в ІКС «Програмна платформа для надання електронних послуг, у тому числі адміністративних».
7. Супровід проведення державної експертизи КСЗІ ІКС.
8. Гарантійний супровід КСЗІ ІКС.

## Перелік нормативно-правових документів, на підставі яких створюється КСЗІ ІКС

Надання послуг зі створення КСЗІ ІКС має відповідати вимогам чинних нормативно-правових документів, а саме:

* Закону України «Про інформацію»;
* Закону України «Про доступ до публічної інформації»;
* Закону України «Про захист інформації в інформаційно-комунікаційних системах»;
* Закону України «Про електронні комунікації»;
* Указу Президента України від 24.09.2001 № 891/2001 «Про деякі заходи щодо захисту державних інформаційних ресурсів у мережах передачі даних»;
* Концепції технічного захисту інформації в Україні, затвердженої постановою Кабінету Міністрів України від 08.10.1997 № 1126;
* Положенню про технічний захист інформації в Україні, затвердженому постановою Кабінету Міністрів України від 27.09.1999 № 1229;
* Положенню про державну експертизу в сфері технічного захисту інформації, затвердженому наказом Адміністрації ДССЗЗІ України від 16.05.2007 № 93, зареєстрованому в Міністерстві юстиції України 16.07.2007 за № 820/14087;
* Положенню про державний контроль за станом технічного захисту інформації, затвердженому наказом Адміністрації ДССЗЗІ України від 16.05.2007 № 87, зареєстрованому в Міністерстві юстиції України 10.07.2007 за № 785/14052;
* Правилам забезпечення захисту інформації в інформаційних, телекомунікаційних та інформаційно-телекомунікаційних системах, затвердженим постановою Кабінету міністрів України від 29.03.2006 № 373;
* Порядку оновлення антивірусних програмних засобів, які мають позитивний експертний висновок за результатами державної експертизи в сфері технічного захисту інформації, затвердженому наказом Адміністрації ДССЗЗІ України від 26.03.2007 № 45, зареєстрованому в Міністерстві юстиції України 10.04.2007 за № 320/13587;
* ДСТУ 2226-93 Автоматизовані системи. Терміни та визначення, затвердженому наказом Держстандарту України від 09.09.93 № 126;
* ДСТУ 3008-2015 Звіти у сфері науки та техніки. Структура та правила оформлювання, затвердженому наказом Держстандарту України від 22.06.2015 № 61 з 2017-07-01;
* НД ТЗІ 1.1-002-99 Загальні положення щодо захисту інформації в комп’ютерних системах від несанкціонованого доступу, затвердженому наказом ДСТСЗІ СБУ від 28.04.1999 № 22;
* НД ТЗІ 1.1-003-99 Термінологія у галузі захисту інформації в комп‘ютерних системах від несанкціонованого доступу, затвердженому наказом ДСТСЗІ СБУ від 28.04.1999 № 22;
* НД ТЗІ 1.4-001-00 Типове положення про службу захисту інформації в автоматизованій системі, затвердженому наказом ДСТСЗІ СБУ від 04.12.2000 № 53;
* НД ТЗІ 2.5-004-99 Критерії оцінки захищеності інформації в комп‘ютерних системах від несанкціонованого доступу, затвердженому наказом ДСТСЗІ СБУ від 28.04.1999 № 22.
* НД ТЗІ 2.5-005-99 Класифікація автоматизованих систем і стандартні функціональні профілі захищеності оброблюваної інформації від несанкціонованого доступу, затвердженому наказом ДСТСЗІ СБУ від 28.04.1999 № 22;
* НД ТЗІ 3.7-001-99 Методичні вказівки щодо розробки ТЗ на створення системи захисту інформації в автоматизованій системі, затвердженому наказом ДСТСЗІ СБУ від 28.04.1999 № 22;
* НД ТЗІ 3.6-001-2000. Технічний захист інформації. Комп’ютерні системи. Порядок створення, впровадження, супроводження та модернізації засобів технічного захисту інформації від несанкціонованого доступу, затвердженому наказом ДСТСЗІ СБУ від 20.12.2000 № 60;
* НД ТЗІ 3.7-003-05 Порядок проведення робіт із створення комплексної системи захисту інформації в інформаційно-телекомунікаційній системі, затвердженому наказом ДСТСЗІ СБУ від 08.11.2005 № 125;
* НД ТЗІ 2.5-008-2002. Вимоги із захисту конфіденційної інформації від несанкціонованого доступу під час оброблення в автоматизованих системах класу 2, затвердженому наказом ДСТСЗІ СБУ від 13.12.2002 № 84;
* НД ТЗІ 2.5-010-03 Вимоги із захисту інформації WEB-сторінки від несанкціонованого доступу, затвердженому наказом ДСТСЗІ СБУ від 02.04.2003 № 33;
* НД ТЗІ 2.6-001-11 Порядок проведення робіт з державної експертизи засобів технічного захисту інформації від несанкціонованого доступу та комплексних систем захисту інформації в інформаційно-телекомунікаційних системах, затвердженому наказом Адміністрації Державної служби спеціального зв’язку та захисту інформації України від 25.03.2011 № 65.

Даний список нормативно-правових документів не є вичерпним. Вимоги законодавства України, нормативних і керівних документів, що стосуються мети та призначення КСЗІ ІКС, мають бути уточнені під час розроблення ТЗ.

# МЕТА, ПРИЗНАЧЕННЯ І ЦІЛІ СТВОРЕННЯ КСЗІ ІКС

## Мета створення КСЗІ ІКС

Мета створення КСЗІ ІКС – досягнення максимальної ефективності захисту за рахунок одночасного цільового використання всіх необхідних ресурсів, методів і засобів, що виключатимуть несанкціонований доступ до інформації, та [створення умов оброблення інформації](http://ndipit.com.ua/ua/poslugy/zahyst-information/neobxidnist-vprovadzhennya) відповідно до вимог чинних нормативно-правових актів України у сфері захисту інформації, а саме: законів України «Про захист інформації в інформаційно-комунікаційних системах», «[Про доступ до публічної інформації](http://zakon1.rada.gov.ua/laws/show/2939-17)» та «[Про захист персональних даних](http://zakon2.rada.gov.ua/laws/show/2297-17)».

## Призначення КСЗІ ІКС

КСЗІ ІКС являє собою сукупність необхідних організаційних та технічних заходів, засобів і методів технічного захисту інформації, спрямованих на недопущення блокування інформації, несанкціонованого доступу до неї та/або її модифікацій.

## Цілі створення КСЗІ ІКС

Цілі створення КСЗІ ІКС:

* забезпечення максимального рівня ефективного захисту інформації в інформаційно-комунікаційної системи «Програмна платформа для надання електронних послуг, у тому числі адміністративних»;
* забезпечення недопущення блокування інформації, несанкціонованого доступу до неї та/або її модифікації в ІКС за рахунок одночасного використання всіх необхідних ресурсів, методів і засобів;
* досягнення максимальної ефективності захисту за рахунок одночасного використання всіх необхідних ресурсів, методів і засобів, що виключають несанкціонований доступ до інформації, та створення умов оброблення інформації відповідно до вимог чинних нормативно-правових актів України у сфері захисту інформації;
* забезпечення можливості безпечного розвитку захищеної ІКС «Програмна платформа для надання електронних послуг, у тому числі адміністративних».

# ВИМОГИ ДО СТВОРЕННЯ КСЗІ ІКС

## Підготовка загальних вимог до КСЗІ ІКС

Підготовка загальних вимог до КСЗІ ІКС повинна базуватися на виконанні таких завдань:

* обґрунтування необхідності створення КСЗІ ІКС, аналіз і визначення наявності у складі інформації, яка підлягає автоматизованому обробленню, таких її видів, що потребують обмеження доступу до неї або забезпечення цілісності чи доступності відповідно до вимог нормативно-правових актів;
* обстеження середовища функціонування КСЗІ ІКС з аналізом та описом ІКС «Програмна платформа для надання електронних послуг, у тому числі адміністративних», інформаційного та фізичного середовища, а також середовища користувачів з метою підготовки вимог до КСЗІ ІКС у вигляді опису кожного середовища функціонування ІКС «Програмна платформа для надання електронних послуг, у тому числі адміністративних» та виявлення в ньому елементів, які безпосередньо чи опосередковано можуть впливати на безпеку інформації, виявлення взаємного впливу елементів різних середовищ, документування результатів обстеження для використання на наступних етапах надання послуг;
* затвердження переліку об’єктів захисту;
* розроблення пропозицій щодо порядку проведення експертних досліджень та формування експертних висновків для ІКС «Програмна платформа для надання електронних послуг, у тому числі адміністративних» з урахуванням можливого розвитку ІКС «Програмна платформа для надання електронних послуг, у тому числі адміністративних», її модернізації та вдосконалення;
* розроблення пропозицій щодо внесення вимог нормативних документів з питань захисту інформації до технічних завдань з розроблення програмного забезпечення інформаційних систем КП ГІОЦ з метою посилення заходів безпеки під час розроблення;
* визначення потенційних загроз для інформації;
* розроблення моделей загроз;
* формування технічних завдань на створення КСЗІ ІКС з урахуванням результатів аналізу ризиків і визначення переліку суттєвих загроз;
* оформлення звітів про виконання робіт та надання заявки на розроблення КСЗІ ІКС.

## Розроблення та оформлення політик безпеки інформації в КСЗІ ІКС, здійснення вибору основних рішень з протидії всім суттєвим загрозам

Політики безпеки розробляються згідно з положеннями НД ТЗІ 1.1-002 та рекомендаціями НД ТЗІ 1.4-001. Політики безпеки рекомендується оформляти у вигляді окремого документа «План захисту».

## Розроблення Технічного завдання на створення КСЗІ ІКС

Розроблення ТЗ має забезпечувати:

* визначення завдання захисту інформації в ІКС «Програмна платформа для надання електронних послуг, у тому числі адміністративних», мети створення КСЗІ ІКС, варіанта вирішення задач захисту, основних напрямів забезпечення захисту;
* здійснення аналізу ризиків (вивчення моделі загроз і моделі порушника, можливих наслідків від реалізації потенційних загроз, величини можливих збитків та інше) і визначення переліку суттєвих загроз;
* визначення загальних структур та складів КСЗІ ІКС, вимог до можливих заходів, методів і засобів захисту інформації, допустимих обмежень щодо застосування певних заходів і засобів, інших обмежень щодо середовищ функціонування ІКС «Програмна платформа для надання електронних послуг, у тому числі адміністративних», обмежень щодо використання ресурсів ІКС «Програмна платформа для надання електронних послуг, у тому числі адміністративних» для реалізації задач захисту, припустимих витрат на створення КСЗІ ІКС, умов створення, введення в дію і функціонування КСЗІ ІКС (окремих її підсистем, компонентів), загальних вимог до співвідношення та меж застосування в ІКС «Програмна платформа для надання електронних послуг, у тому числі адміністративних» (окремих її підсистем, компонентів) організаційних, інженерно-технічних, технічних, криптографічних та інших заходів захисту інформації, що увійдуть до складу КСЗІ ІКС.

## Розроблення проєкту КСЗІ ІКС

Розроблення проєкту КСЗІ ІКС має забезпечувати виконання таких завдань:

1. Розроблення техноробочого проєкту КСЗІ ІКС з відповідним пакетом документації.
2. Розроблення нормативно-розпорядчої документації КСЗІ ІКС:

* посадових (функціональних) інструкцій фахівців СЗІ, адміністраторів, персоналу та користувачів ІКС «Програмна платформа для надання електронних послуг, у тому числі адміністративних»;
* технологічних (операційних) інструкцій (настанов) щодо виконання завдань з адміністрування та обслуговування КСЗІ ІКС (згідно з НД ТЗІ 2.6-001-2011).

1. Розроблення документації до проведених випробувань КСЗІ ІКС:

* «Програми та методики випробувань комплексної системи захисту інформації для інформаційно-комунікаційної системи «Програмна платформа для надання електронних послуг, у тому числі адміністративних»;
* протоколу попередніх випробувань КСЗІ ІКС зі звітом з випробувань.

1. Розроблення організаційно-розпорядчої документації КСЗІ ІКС:

* проєкту наказу про створення КСЗІ ІКС;
* проєкту наказу про створення служби захисту інформації;
* проєкту наказу про призначення комісії для проведення попередніх випробувань КСЗІ ІКС;
* проєкту наказу про створення комісії для приймання КСЗІ ІКС у дослідну експлуатацію;
* проєкту акта про приймання КСЗІ ІКС в дослідну експлуатацію;
* проєкту акта про завершення дослідної експлуатації КСЗІ ІКС;
* проєкту акта про завершення робіт зі створення КСЗІ ІКС.

1. Розроблення супровідної документації КСЗІ ІКС:

* формуляра;
* реєстраційного журналу, використовуваних для реєстрації фактів і результатів виконання певних завдань з адміністрування та обслуговування КСЗІ ІКС.

## Введення КСЗІ ІКС в дію та оцінювання захищеності інформації в ІКС «Програмна платформа для надання електронних послуг, у тому числі адміністративних»

Введення КСЗІ ІКС в дію та оцінювання захищеності інформації в ІКС «Програмна платформа для надання електронних послуг, у тому числі адміністративних» мають відповідати таким завданням та задовольняти такі вимоги:

* надання послуг з підготовки організаційних структур та розроблення розпорядчих документів, що регламентують діяльність із забезпечення захисту інформації в ІКС «Програмна платформа для надання електронних послуг, у тому числі адміністративних»;
* проведення попередніх випробувань згідно з «Програмою та методикою випробувань», перевірка працездатності КСЗІ ІКС та визначення можливості прийняття їх у дослідну експлуатацію, оформлення протоколів випробувань;
* проведення дослідної експлуатації, під час якої відпрацьовуються технології оброблення інформації, обігу машинних носіїв інформації, керування засобами захисту, розмежування доступу користувачів до ресурсів ІКС «Програмна платформа для надання електронних послуг, у тому числі адміністративних» та автоматизованого контролю за діями користувачів;
* супровід проведення державної експертизи КСЗІ ІКС з метою визначення відповідності КСЗІ ІКС ТЗ вимогам НД ТЗІ із захисту інформації та визначення можливості введення КСЗІ ІКС в експлуатацію;
* усунення недоліків у разі їх виявлення під час проведення державної експертизи.

## Супровід КСЗІ ІКС

Виконавець упродовж строку дії Атестата відповідності повинен забезпечити гарантійну підтримку (супровід) КСЗІ ІКС Замовника, що включає актуалізацію документації КСЗІ ІКС Замовника та надання інформаційно-консультаційної підтримки щодо експлуатації КСЗІ ІКС за запитом Замовника.

# СКЛАД І ЗМІСТ ПОСЛУГ ЗІ СТВОРЕННЯ КСЗІ ІКС

Послуги з розроблення КСЗІ ІКС мають надаватися за етапами.

**1-й етап. Підготовка загальних вимог до КСЗІ ІКС, розроблення та оформлення політик безпеки інформації, здійснення вибору основних рішень з протидії всім суттєвим загрозам, обстеження середовища функціонування ІКС «Програмна платформа для надання електронних послуг, у тому числі адміністративних», розроблення пропозицій щодо забезпечення можливості розвитку/модернізації захищених систем, розроблення ТЗ та узгодження ТЗ з ДССЗЗІ.**

Під час цього етапу виконується:

1. Підготовка загальних вимог до КСЗІ ІКС.

Визначення наявності у складі інформації, яка підлягає автоматизованому обробленню, таких її видів, що потребують обмеження доступу до неї або забезпечення цілісності чи доступності відповідно до вимог нормативно-правових актів.

1. Підготовка організаційно-розпорядчої документації.

Фахівці Виконавця проводять аналіз організаційно-розпорядчих документів Замовника і нормативно-правових документів в області захисту інформації, що впливають на діяльність Замовника.

За результатами проведеного аналізу Виконавець, ураховуючи вимоги законодавчих актів України у сфері захисту інформації, готує проєкти документів, які визначають організаційну складову КСЗІ:

* проєкт «Положення про службу захисту інформації»;
* проєкти посадових інструкцій фахівців служби захисту інформації;
* проєкт наказу КП ГІОЦ про створення служби захисту інформації,   
  які затверджуються Замовником.

1. Обстеження середовищ функціонування ІКС «Програмна платформа для надання електронних послуг, у тому числі адміністративних».

Метою обстеження є підготовка Виконавцем засадничих даних для формування вимог до КСЗІ ІКС у вигляді опису середовищ функціонування ІКС «Програмна платформа для надання електронних послуг, у тому числі адміністративних» та виявлення в ньому елементів, які безпосередньо чи опосередковано можуть впливати на безпеку інформації, виявлення взаємного впливу елементів різних середовищ, документування результатів обстеження для використання на наступних етапах послуг.

Під час обстеження Виконавцем ІКС «Програмна платформа для надання електронних послуг, у тому числі адміністративних» мають бути уточнені, проаналізовані й описані:

* загальна структурна схема і склад (перелік і склад обладнання, технічних і програмних засобів, їхні зв’язки, особливості конфігурації, архітектури й топології, програмні і програмно-апаратні засоби захисту інформації, взаємне розміщення засобів тощо);
* види і характеристики каналів зв’язку;
* особливості взаємодії окремих компонентів, їх взаємний вплив один на одного;
* можливі обмеження щодо використання засобів та інше.

Виконавцем мають бути виявлені компоненти обчислювальної системи, які містять і які не містять засобів і механізмів захисту інформації, потенційні можливості цих засобів і механізмів, їхні властивості й характеристики, в тому числі такі, що встановлюються за замовчуванням тощо.

Метою такого аналізу є формування Виконавцем загального уявлення про наявність потенційних можливостей щодо забезпечення захисту інформації, виявлення компонентів ІКС «Програмна платформа для надання електронних послуг, у тому числі адміністративних», які вимагають підвищених вимог до захисту інформації і впровадження додаткових заходів захисту.

В результаті аналізу Виконавцем технології оброблення інформації мають бути визначені й описані інформаційні потоки і середовища, через які вони передаються, джерела утворення потоків і місця їх призначення, принципи та методи керування інформаційними потоками, складені структурні схеми потоків. Фіксуються види носіїв інформації та порядок їх використання під час функціонування ІКС «Програмна платформа для надання електронних послуг, у тому числі адміністративних».

Для кожного структурного елемента схеми інформаційних потоків Виконавцем фіксуються склад інформаційних об’єктів, режим доступу до них, можливий вплив на нього елементів (елемента) середовища користувачів, фізичного середовища з точки зору збереження властивостей інформації.

Під час обстеження фізичного середовища Виконавцем здійснюється аналіз взаємного розміщення засобів оброблення інформації ІКС «Програмна платформа для надання електронних послуг, у тому числі адміністративних» на об’єктах інформаційної діяльності, комунікацій, систем життєзабезпечення і зв’язку, а також режим функціонування цих об’єктів.

Порядок проведення обстеження повинен відповідати ДСТУ 3396.1.

Аналізу мають підлягати такі характеристики фізичного середовища:

* територіальне розміщення компонентів ІКС «Програмна платформа для надання електронних послуг, у тому числі адміністративних»;
* наявність охорони території та пропускний режим;
* наявність і стан приміщень, у яких мають розміщуватися компоненти ІКС «Програмна платформа для надання електронних послуг, у тому числі адміністративних»;
* режим доступу до компонентів фізичного середовища ІКС «Програмна платформа для надання електронних послуг, у тому числі адміністративних»;
* наявність і технічні характеристики систем забезпечення (клімат, живлення, заземлення тощо);
* наявність проєктної та експлуатаційної документації.

Під час обстеження Виконавцем середовища користувачів здійснюється аналіз:

* функціонального та кількісного складу користувачів, їхніх функціональних обов’язків, виробничого навантаження та рівня кваліфікації;
* повноважень користувачів щодо допуску до управління елементами ІКС «Програмна платформа для надання електронних послуг, у тому числі адміністративних», у тому числі повноважень користувачів щодо управління КСЗІ;
* рівня необхідних прав і можливостей різних категорій користувачів, які повинні мати права доступу до інформації ІКС «Програмна платформа для надання електронних послуг, у тому числі адміністративних»;
* наявність служби захисту інформації в ІКС «Програмна платформа для надання електронних послуг, у тому числі адміністративних» .

Результати обстеження середовищ функціонування ІКС «Програмна платформа для надання електронних послуг, у тому числі адміністративних» повинні бути оформлені Виконавцем у вигляді акта.

За результатами обстеження середовищ функціонування ІКС «Програмна платформа для надання електронних послуг, у тому числі адміністративних» Виконавцем має бути визначений перелік об’єктів захисту (з урахуванням рекомендацій НД ТЗІ 1.4-001, НД ТЗІ 2.5-007, НД ТЗІ 2.5-008, НД ТЗІ 2.5-010 щодо класифікації об’єктів), а також визначені потенційні загрози для інформації і розроблені модель загроз та модель порушника. Побудова моделей повинна здійснюватися відповідно до положень НД ТЗІ 1.1-002, НД ТЗІ 1.4-001 та НД ТЗІ 1.6-003.

За результатами обстеження інформаційної інфраструктури ІКС «Програмна платформа для надання електронних послуг, у тому числі адміністративних» Виконавець розробляє та погоджує із Замовником такі документи:

* «Пропозиції щодо порядку проведення експертних досліджень та формування експертних висновків в ІКС ГІОЦ з урахуванням розвитку інформаційних систем КП ГІОЦ, їх модернізації та вдосконалення. Звіт за результатами обстеження інформаційної інфраструктури КП ГІОЦ»;
* «Пропозиції щодо внесення вимог нормативних документів з питань захисту інформації до технічних завдань з розроблення програмного забезпечення ІКС КП ГІОЦ з метою посилення заходів безпеки під час розроблення. Звіт за результатами ознайомлення з документацією на ІКС «Програмна платформа для надання електронних послуг, у тому числі адміністративних».

Документи оформляються у відповідності до вимог ДСТУ 3008-2015 Звіти у сфері науки та техніки. Структура та правила оформлювання, затвердженого наказом Держстандарту України від 22.06.2015 № 61 з 2017-07-01.

1. Розроблення Технічного завдання на створення КСЗІ ІКС.

Виконавець розробляє і погоджує із Замовником документ «Технічне завдання на створення комплексної системи захисту інформації для інформаційно-комунікаційної системи «Програмна платформа для надання електронних послуг, у тому числі адміністративних», яке визначає всі основні вимоги до КСЗІ ІКС й можливі варіанти реалізації її складових елементів. Після узгодження Технічного завдання на створення комплексної системи захисту інформації для інформаційно-комунікаційної системи «Програмна платформа для надання електронних послуг, у тому числі адміністративних» із Замовником документ узгоджується з ДССЗЗІ. Відповідно до п 5.1 НД ТЗІ 3.7-001-99 допускається оформлення вимог до захисту інформації у вигляді окремого (часткового) ТЗ, доповнення до загального ТЗ або розділу загального ТЗ.

1. Розроблення пакету документів «План захисту інформації».

Виконавець розробляє пакет документів «План захисту інформації» в такому складі:

* «Модель загроз інформації. Модель порушника»;
* «Положення про Службу захисту інформації»;
* «Політика безпеки інформації в ІКС «Програмна платформа для надання електронних послуг, у тому числі адміністративних»,

які затверджуються Замовником.

Загальний перелік документів, які створюються за цим етапом:

1. Проєкт «Положення про службу захисту інформації».
2. Проєкти посадових інструкцій фахівців служби захисту інформації.
3. Проєкт наказу КП ГІОЦ про створення служби захисту інформації.
4. Акт обстеження середовищ функціонування ІКС «Програмна платформа для надання електронних послуг, у тому числі адміністративних».
5. «Пропозиції щодо порядку проведення експертних досліджень та формування експертних висновків в ІКС ГІОЦ з урахуванням розвитку інформаційних систем КП ГІОЦ, їх модернізації та вдосконалення. Звіт за результатами обстеження інформаційної інфраструктури КП ГІОЦ».
6. «Пропозиції щодо внесення вимог нормативних документів з питань захисту інформації до технічних завдань з розроблення програмного забезпечення ІКС КП ГІОЦ з метою посилення заходів безпеки під час розроблення».
7. Звіт за результатами ознайомлення з документацією на ІКС «Програмна платформа для надання електронних послуг, у тому числі адміністративних».
8. «Технічне завдання на створення комплексної системи захисту інформації для інформаційно-комунікаційної системи «Програмна платформа для надання електронних послуг, у тому числі адміністративних».
9. «Модель загроз інформації. Модель порушника»;
10. «Політика безпеки інформації в ІКС «Програмна платформа для надання електронних послуг, у тому числі адміністративних».

**2-й етап. Розроблення проєкту КСЗІ ІКС**

Під час цього етапу виконується:

1. Розроблення техноробочого проєкту на створення КСЗІ ІКС.

Після узгодження ТЗ з ДССЗЗІ Виконавець розробляє пакет документів техноробочого проєкту на створення КСЗІ ІКС.

Техноробочий проєкт на створення КСЗІ ІКС є комплектом документів, до якого входить частина документів, розроблених на попередніх етапах і низка нових документів, у яких описано, як саме створюватиметься, експлуатуватиметься і, за потреби, модернізуватиметься КСЗІ ІКС.

Техноробочий проєкт на створення КСЗІ ІКС розробляється на підставі Технічного завдання на створення КСЗІ ІКС. Виконавцем повинні здійснюватися розроблення, оформлення, узгодження та затвердження документації в обсязі, передбаченому ТЗ. Зміст і стиль документації мають бути достатніми для повного опису проєктних рішень рівня технічного проєкту. Під час розроблення проєкту КСЗІ ІКС обґрунтовуються і приймаються проєктні рішення, які дають можливість реалізувати вимоги ТЗ, забезпечити сумісність і взаємодію різних компонентів КСЗІ ІКС, а також різних заходів і способів захисту інформації.

В результаті створюється комплект робочої та експлуатаційної документації, необхідної для забезпечення випробування, проведення пусконалагоджувальних робіт, випробувань та управління КСЗІ ІКС.

Техноробочий проєкт на створення КСЗІІКСмає включати такий пакет документів:

* інструкції з експлуатації КСЗІ ІКС та її елементів;
* процедури регламентного обслуговування КСЗІ ІКС;
* правила і положення проведення випробувань і аналізу роботи КСЗІ ІКС;
* керівництва адміністраторів і користувачів;
* формуляр КСЗІ ІКС.

Вимоги до документації та методичного забезпечення щодо першого та другого етапів можуть бути уточнені в ТЗ.

**3й етап. Введення КСЗІ ІКС у дію та оцінювання захищеності інформації в ІКС «Програмна платформа для надання електронних послуг, у тому числі адміністративних»**

Під час цього етапу виконується:

1. Приведення інформаційної інфраструктури Замовника у відповідність до техноробочого проєкту на створення КСЗІ ІКС.

Проводиться приведення інформаційної інфраструктури Замовника у відповідність до техноробочого проєкту на створення КСЗІ ІКС.

Має бути створено СЗІ (призначення осіб, відповідальних за захист інформації). Виконавцем має бути завершено розроблення, а також подані Замовнику на затвердження документи, що входять до плану захисту (за виключенням тих, для розроблення яких необхідні результати наступних етапів послуг). Виконавець надає Замовнику проєкт наказу про створення комісії та проведення попередніх випробувань, проєкт наказу про створення комісії та проведення дослідної експлуатації.

Створення СЗІ та розроблення плану захисту мають бути здійснені Виконавцем згідно з НД ТЗІ 1.4-001.

1. Проведення пусконалагоджувальних робіт та навчання користувачів.

Виконавець проводить усі пусконалагоджувальні роботи, навчання та інструктажі персоналу (до 5 фахівців) Замовника згідно з правилами і режимами експлуатації КСЗІ ІКС.

Проводяться такі заходи:

* організація захисту інформації від несанкціонованого доступу (НСД);
* організація антивірусного захисту інформації;
* розроблення «Програми і методики випробувань комплексної системи захисту інформації для інформаційно-комунікаційної системи «Програмна платформа для надання електронних послуг, у тому числі адміністративних»;
* проведення попередніх випробувань.

1. Випробування КСЗІ ІКС.

Проводяться попередні випробування КСЗІ ІКС з метою підтвердження результативності її роботи і відповідності вимогам, визначеним у Технічному завданні на створення КСЗІ ІКС. У процесі випробувань виконуються тестові завдання і контролюються отримані результати, які і є індикатором працездатності спроєктованої КСЗІ ІКС.

Попередні випробування мають бути проведені Виконавцем згідно з «Програмою та методикою випробувань комплексної системи захисту інформації для інформаційно-комунікаційної системи «Програмна платформа для надання електронних послуг, у тому числі адміністративних», надалі – «Програма та методика випробувань». Документ «Програма та методика випробувань» готує Виконавець, а узгоджує Замовник.

За результатом попереднього випробування КСЗІ ІКС робиться висновок відносно можливості прийняття КСЗІ ІКС у дослідну експлуатацію.

1. Проведення дослідної експлуатації.

Проводиться дослідна експлуатація, під час якої:

* відпрацьовуються технології оброблення інформації, облік машинних носіїв інформації, управління засобами захисту, розмежування доступу користувачів до ресурсів ІКС «Програмна платформа для надання електронних послуг, у тому числі адміністративних» і автоматизованого контролю за діями користувачів;
* фахівці служби захисту інформації і користувачі ІКС «Програмна платформа для надання електронних послуг, у тому числі адміністративних» набувають практичних навичок використання технічних і програмно-апаратних засобів захисту інформації, засвоюють вимоги організаційних і розпорядчих документів з питань розмежування доступу до технічних засобів й інформаційних ресурсів;
* здійснюється (за необхідності) доопрацювання програмного забезпечення, додаткове налагодження та конфігурування КЗЗ;
* здійснюється (за необхідності) коригування робочої та експлуатаційної документації.

За результатами дослідної експлуатації приймається рішення щодо готовності КСЗІ ІКС до подання на державну експертизу.

**4-й етап. Супровід проведення державної експертизи КСЗІ ІКС і отримання «Атестата відповідності»**

Надання послуг із супроводу проведення державної експертизи КСЗІ ІКС і отримання «Атестата відповідності» складається з:

* підготовки КСЗІ ІКС до проведення державної експертизи в ДССЗЗІ й супроводу експертних випробувань;
* узгодження з ДССЗЗІ результатів експертизи і видача Замовникові «Атестата відповідності».

Державна експертиза проводиться з метою визначення відповідності КСЗІ ІКС вимогам ТЗ, вимогам нормативної документації до захисту інформації і визначення можливості введення КСЗІ ІКС в експлуатацію.

В разі виявлення недоліків під час проведення державної експертизи, їх усунення здійснюється до завершення державної експертизи. Порядок усунення виявлених недоліків такий самий, як і для попередніх випробувань. Якщо усунути недоліки в ході експертизи неможливо, складається акт, до якого вноситься перелік необхідних доробок та рекомендації щодо їх виконання. Після завершення робіт, передбачених актом, проводиться повторна експертиза.

В межах заходів з організації та проведення державної експертизи КСЗІ ІКС Виконавець повинен забезпечити надання таких послуг:

* попередній аналіз стану забезпечення захисту ІКС та реалізованих організаційно-технічних й організаційних заходів;
* внесення змін до організаційно-технічних заходів впровадження КСЗІ ІКС (за необхідності), актуалізація стану, підготовка додаткової інформації щодо ІКС «Програмна платформа для надання електронних послуг, у тому числі адміністративних», коригування впроваджених організаційно-технічних заходів відповідно до зауважень і рекомендацій експерта;
* розроблення та погодження із Замовником та уповноваженим структурним підрозділом Адміністрації ДССЗЗІ програми проведення експертних випробувань КСЗІ ІКС;
* розроблення та погодження з уповноваженим структурним підрозділом Адміністрації ДССЗЗІ методики проведення експертних випробувань КСЗІ ІКС;
* оформлення результатів проведення експертних випробувань КСЗІ ІКС відповідними протоколами та проєктом експертного висновку на КСЗІ ІКС, який узгоджується з ДССЗЗІ.

|  |  |
| --- | --- |
| **ЗАМОВНИК** | **ВИКОНАВЕЦЬ** |
| **Комунальне підприємство «Головний інформаційно-обчислювальний центр»** |  |
| **\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_**  **м. п.** | **\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_**  **м. п.** |