***ДОДАТОК 3***

*до тендерної документації*

**ПРОЄКТ**

**ДОГОВІР №\_\_\_\_\_\_\_**

**про надання послуг**

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

**Державна установа «Агентство з розвитку інфраструктури фондового ринку України»** (надалі – Замовник) 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-\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_:

**Послуги зі створення комплексної системи захисту інформації для інформаційно-комунікаційної системи: «SMIDA+»,** керуючись Цивільним кодексом України, Господарським кодексом України, Законом України «Про публічні закупівлі» та іншими нормативно-правовими актами України, уклали цей Договір про надання послуг (надалі – Договір) про нижченаведене.

1. **ПРЕДМЕТ ДОГОВОРУ**
   1. Виконавець зобов’язується в порядку та на умовах, визначених Договором, надати Замовнику послуги зі створення комплексної системи захисту інформації для інформаційно-комунікаційної системи: «SMIDA+» (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. Технічні та інші вимоги до послуг визначаються в Інформації про необхідні технічні, якісні, кількісні та інші характеристики предмету договору (Технічні вимоги), що є Додатком 2 до Договору, який є невід’ємною частиною Договору, далі – Технічні вимоги.
2. **ЯКІСТЬ ПОСЛУГ ТА ГАРАНТІЙНІ ЗОБОВ’ЯЗАННЯ**
   1. Виконавець повинен мати відповідні дозволи, ліцензії і сертифікати для надання таких Послуг. Виконавець повинен надати Замовнику послуги, якість яких відповідає Технічним вимогам (Додаток 2 до цього Договору) та 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 (супроводження) комплексної системи захисту інформації для інформаційно-комунікаційної системи: «SMIDA+» (далі – КСЗІ ІКС), що включає надання інформаційно-консультаційної підтримки щодо експлуатації КСЗІ ІКС за запитом Замовника, впродовж 12 (дванадцяти) місяців з дати підписання Сторонами Акту 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 та/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 могли 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. Ціна послуг за кожним етапом надання послуг зазначена в Календарному плані.
   3. Розрахунки за надані послуги здійснюються в національній валюті України – гривні, шляхом перерахування Замовником грошових коштів на поточний рахунок Виконавця протягом 20 (двадцяти) робочих днів після підписання Сторонами Акту приймання-передачі наданих послуг за відповідним етапом.
   4. Ціна Договору може бути змінена у випадках, передбачених статтею 41 Закону України «Про публічні закупівлі».
4. **ПОРЯДОК І СТРОКИ НАДАННЯ ПОСЛУГ**
   1. Місце надання послуг: м. Київ, Антоновича, 51, оф. 1206. Строки надання послуг: відповідно до Календарного плану, але в будь-якому випадку не пізніше «25» грудня 2023 року.
   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 в паперовому вигляді, а також документацію, яка передбачена умовами договору згідно з Календарним планом та технічних вимог, в електронному вигляді на змінному електронному носієві інформації (у вигляді цифрових файлів) та в паперовому вигляді.
   6. Приймання та оцінка наданих послуг за відповідним етапом здійснюється впродовж 7 (семи) робочих днів з дати надання Виконавцем Замовнику Акту приймання-передачі наданих послуг Замовником. У разі виявлення Замовником невідповідностей наданих послуг вимогам Договору 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.
5. **ПРАВА ТА ОБОВ'ЯЗКИ СТОРІН**
   1. *Замовник зобов’язаний:*
      1. Своєчасно та в повному обсязі сплачувати вартість належним чином наданих послуг.
      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.
   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 фінансування видатків 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 частиною п’ятою статті 41 Закону України «Про публічні закупівлі».
  + 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. Мати всі права (дозволи, ліцензії, сертифікати, тощо) та правові підстави, необхідні для виконання своїх зобов'язань за Договором та наданням Послуг визначених в Технічних вимогах (Додаток 2 до цього Договору).
     2. Надати Замовнику послуги за відповідним етапом у строки, встановлені Договором, в тому числі Календарним планом.
     3. Забезпечити надання послуг, якість та комплектність яких відповідає умовам, встановленим Договором, в тому числі Технічним вимогам.
     4. Дотримуватись робочого розпорядку, що діє у Замовника, правил охорони праці та пожежної безпеки під час перебування на території Замовника.
     5. За свій рахунок виконувати гарантійні зобов’язання протягом гарантійного строку на умовах, встановлених Договором.
     6. 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 приховування 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.
     7. 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 надання, за кожний день прострочення.
   3. У разі якщо прострочення встановлених строків надання послуг за етапом перевищує 15 (п’ятнадцять) календарних днів Виконавець додатково сплачує Замовнику штраф у розмірі 10 % (десяти відсотків) від вартості послуг, з яких допущено прострочення. Сплата пені, штрафу відбувається шляхом утримання Змовником грошових коштів з суми коштів, що належить до перерахування Виконавцю відповідно до п.3.3. Договору.
   4. Збитки, завдані Замовнику неналежним виконанням Виконавцем зобов’язань за Договором, підлягають відшкодуванню у повній сумі понад встановлені Договором штрафні санкції.
   5. 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 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 укладання 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 телекомунікацій 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.
   5. Даний Договір укладається між Сторонами в період дії форс-мажорних обставин, що підтверджується документом Торгово-Промислової палати України від 28.02.2022   
      |№2024/02.0-7.1.Сторони зобов’язуються здійснювати всі залежні від них дії для повного та своєчасного виконання взятих на себе зобов’язань за цим Договором, але в разі, якщо такі вже наявні форс-мажорні обставини (в тому числі бойові дії, припинення сполучення між містами, мобілізація або загибель співробітників, тощо) унеможливлять виконання таких зобов’язань, Сторони звільняються від відповідальності за таке невиконання.
   6. 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.
2. **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.
3. **СТРОК ДІЇ ДОГОВОРУ**
   1. Договір набирає чинності з дати його підписання і діє до 31 грудня 2023 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. Дія Договору може продовжуватися на строк, достатній для проведення процедури закупівлі на початку наступного року, в обсязі, що не перевищує 20 відсотків суми, визначеної в Договорі, якщо видатки на цю мету затверджено в установленому порядку.
4. **АНТИКОРУПЦІЙНІ ПОЛОЖЕННЯ ТА ЗАСТЕРЕЖЕННЯ**
   1. Під час виконання своїх зобов’язань за цим Договором Сторони, їхні афілійовані особи, працівники або уповноважені представники, прямо або опосередковано, не виплачують та не надають, не обіцяють, не пропонують, не погоджують виплату/надання грошових коштів або майна, нематеріальних активів, переваг, пільг, послуг чи інших вигод матеріального чи нематеріального характеру будь-яким особам з метою впливу на дії чи рішення цих осіб чи отримання будь-яких неправомірних переваг чи досягнення інших неправомірних цілей.
   2. Під час виконання своїх зобов’язань за цим Договором Сторони, їхні афілійовані особи, працівники або уповноважені представники не вчиняють будь-які дії, які можуть кваліфікуватися як надання/отримання неправомірної вигоди, корупційне правопорушення, а також дії, що порушують вимоги чинного законодавства про запобігання корупції та міжнародних актів про протидію легалізації (відмиванню) доходів, одержаних злочинним шляхом.
   3. Кожна із Сторін цього Договору відмовляється від стимулювання будь-яким чином представників іншої Сторони, у тому числі шляхом надання грошових сум, подарунків, безоплатного виконання робіт, надання послуг чи іншими способами, що ставлять представника в певну залежність і спрямовані на забезпечення виконання цим представником будь-яких дій на користь стимулюючої його Сторони.
   4. У разі виявлення фактів або підозр про порушення умов даного Антикорупційного застереження в процесі виконання цього Договору Постачальник зобов’язується негайно повідомити за номером телефону Гарячої лінії Покупця  +38 (044) 586-43-93 або надати відповідну інформацію на електронну адресу [anticor@smida.gov.ua](mailto:anticor@smida.gov.ua)
   5. Покупець має право в односторонньому порядку відмовитися від виконання своїх зобов’язань за Договором та/або розірвати Договір у випадку порушення будь-яких зобов’язань, наданих Постачальником у пунктах 1-3 цього антикорупційного застереження.

.

1. **КОНФІДЕНЦІЙНІСТЬ**
   1. Виконавець зобов'язується зберігати конфіденційність усієї інформації (у тому числі документів і контактної інформації), отриманої від Замовника або за сприяння Замовника, або до якої у Виконавця є доступ у зв'язку з виконанням ним своїх зобов'язань за Договором, а також інформації про умови Договору та не розкривати її без попередньої письмової згоди Замовника будь-якій особі, крім Замовника або вказаних ним осіб.
   2. Під Інформацією розуміється, інформація яка:

- зберігається в письмовій, електронній або в будь-якій іншій матеріальній формі і 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-телекомунікаційних системах тощо);

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

Сторони гарантують, що надання та отримання персональних даних, інші можливі дії з такими даними у зв’язку з виконанням цього Договору будуть здійснюватися Сторонами при повному дотриманні ними законодавства України про захист персональних даних, зокрема Закону України “Про захист персональних даних”.

* 1. Виконавець зобов'язується протягом строку дії цього Договору та протягом 5 (п’яти) років після його припинення забезпечити захист конфіденційної інформації, отриманої від Замовника та за сприяння Замовника в рамках цього Договору, або до якої у Виконавця є доступ у зв'язку з виконанням ним своїх зобов'язань за цим Договором, і не використовувати цю інформацію для цілей, не пов'язаних з виконанням зобов'язань за цим Договором.
  2. Виконавець гарантує, що дані зобов'язання будуть дотримуватися усіма особами, що залучаються ним до виконання цього Договору, включаючи працівників Виконавця і будь-яких субпідрядників.
  3. Щоб уникнути виникнення спірних ситуацій до конфіденційної інформації не відноситься інформація, яка:

- вже знаходиться у відкритому доступі;

- розкрита іншій Стороні без пред'явлення будь-яких вимог щодо дотримання конфіденційності третьою стороною, яка отримала її або безпосередньо, або опосередковано від її власника;

- є або стає загальнодоступною не через дії або невиконання своїх зобов'язань Виконавцем, або працівниками Виконавця;

- повинна бути розкрита згідно чинного законодавства або на законну вимогу державних органів влади за умови повідомлення іншої Сторони про отримання офіційного письмового документу (відповідного запиту, вимоги, протокол про виїмку тощо) та/або нормативний акт, згідно якого/их відбулося розкриття, або відразу після його отримання і, наскільки це можливо, до такого розкриття.

* 1. Будь-яка інформація, за винятком інформації, зазначеної у п. 11.5 цього Договору, отримана від Покупця або за його сприяння, або яка стала доступна Виконавцю під час виконання цього Договору, є конфіденційною незалежно від наявності або відсутності вимоги Замовника або його представника щодо конфіденційності інформації, наявності на носії інформації будь-якого грифу конфіденційності, форми, або способу передачі інформації, змісту інформації та носія інформації.
  2. 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 УМОВИ**
   1. Істотні умови Договору не можуть змінюватися після його підписання до виконання зобов’язань Сторонами в повному обсязі, крім випадків, передбачених статтею 41 Закону України «Про публічні закупівлі».
   2. Жодна із Сторін не має права передавати свої права та обов’язки за Договором третім особам без письмової згоди на те іншої Сторони.
   3. Всі письмові повідомлення, передбачені Договором, направляються за адресами, вказаними в Договорі, рекомендованою поштою з повідомленням про вручення, службою кур’єрської доставки або вручаються представникам Сторін особисто під розпис.
   4. Підписуючи Договір, уповноважені представники Сторін дають згоду (дозвіл) на обробку їх персональних даних, з метою підтвердження повноважень суб’єкта на укладання, зміну та розірвання Договору, а також для забезпечення реалізації адміністративно-правових і податкових відносин, відносин у сфері бухгалтерського обліку та статистики, а також для забезпечення реалізації інших передбачених законодавством відносин. Представники Сторін підписанням цього Договору підтверджують, що вони повідомлені про свої права відповідно до статті 8 Закону України «Про захист персональних даних».
   5. 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).
   6. 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.
   7. Умови Договору можуть бути змінені за згодою Сторін у порядку, визначеному законодавством України, шляхом укладання 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.
   8. 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.
   9. Про зміни реквізитів, установчих документів, організаційно-правової форми тощо Сторони у письмовій формі зобов’язані протягом 7 (семи) робочих днів повідомити одна одну.
   10. Виконавець є платником \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_.
   11. Замовник є платником податку на прибуток підприємств на загальних підставах.
2. **ДОДАТКИ ДО ДОГОВОРУ**
   1. Невід’ємними частинами Договору є:
      1. Додаток 1 – Календарний план надання послуг.
      2. Додаток 2 – Інформація про необхідні технічні, якісні, кількісні та інші характеристики предмета Договору (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.
3. **РЕКВІЗИТИ СТОРІН**

|  |  |
| --- | --- |
| **ЗАМОВНИК** | **ВИКОНАВЕЦЬ** |
| **Державна установа «Агентство з розвитку інфраструктури фондового ринку України»** |  |
| **\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_**  **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: «SMIDA+»**

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| **№**  **з/п** | **Назва етапу** | **Строк виконання** | **Документація, що надається за етапом** | **Обсяг фінансування від загальної ціни договору, %** | **Вартість етапу, грн. у т.ч. ПДВ** |
| 1 | Обстеження середовища функціонування ІКС та розробка ТЗ на КСЗІ ІКС. Узгодження ТЗ з ДССЗЗІ | 35 робочих днів з дати укладення Договору | 1. Акт обстеження середовищ функціонування ІКС. 2. Перелік інформації, що підлягає автоматизованому обробленню в ІКС та потребує захисту. 3. Модель загроз інформації. Модель порушника. 4. Політика безпеки інформації. 5. Положення про Службу захисту інформації. 6. Технічне завдання, узгоджене з ДССЗЗІ. 7. Акт приймання –передачі робіт по за етапом 1. | 35 |  |
| 2 | Проектування КСЗІ ІКС | 20 робочих днів з дати завершення 1 етапу | 1. Документація техноробочого проекту 2. Акт приймання –передачі робіт по за етапом 2. | 20 |  |
| 3 | Впровадження КСЗІ ІКС | 20 робочих днів з дати завершення 2 етапу | 1. Програма та методика проведення попередніх випробувань КСЗІ ІКС. 2. Проект протоколу проведення попередніх випробувань КСЗІ ІКС. 3. Проект акту про прийняття в дослідну експлуатацію КСЗІ ІКС. 4. Проект акту завершення дослідної експлуатації КСЗІ ІКС. 5. Проект акту завершення робіт зі створення КСЗІ ІКС 6. Звіт про проведення навчання користувачів та комплектування КСЗІ ІКС. 7. Паспорт (формуляр) КСЗІ ІКС. 8. План захисту інформації. 9. Проект заявки на проведення державної експертизи КСЗІ. 10. Акт приймання –передачі робіт по за етапом 3. | 15 |  |
| 4 | Супровід проведення державної експертизи КСЗІ ІКС та отримання "Атестата відповідності" | 30 робочих днів з дати завершення 3 етапу | 1. Атестат відповідності, зареєстрований Держспецзв’язку. 2. Експертний висновок, який додається до Атестата відповідності та є його невід’ємною частиною. 3. Акт приймання –передачі робіт по за етапом 4. | 30 |  |
| **Загальна вартість етапів (всього), грн. у т.ч. ПДВ** | | | | |  |

*Виконавець забезпечує інформування Замовника про завершення всіх підготовчих робіт та можливості подання заявки на проведення державної експертизи. Відповідно до п. 6.5.8.7 НД ТЗІ 3.7-003-2005 допускається розпочинати і проводити державну експертизу КСЗІ паралельно з роботами етапів проектування.*

|  |  |
| --- | --- |
| **ЗАМОВНИК** | **ВИКОНАВЕЦЬ** |
| **Державна установа «Агентство з розвитку інфраструктури фондового ринку України»** |  |
| **\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_**  **м. п.** | **\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_**  **м. п.** |

Додаток 2

до Договору №\_\_\_\_\_\_

про надання послуг

від \_\_\_\_\_\_\_\_\_\_\_\_2023 року

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

**(ТЕХНІЧНІ ВИМОГИ)**

**Послуги зі створення комплексної системи захисту інформації дляінформаційно-комунікаційної системи: «SMIDA+»**

**1. ЗАГАЛЬНІ ВІДОМОСТІ**

* 1. **Загальні положення, терміни, визначення та скорочення**

|  |  |
| --- | --- |
| Виконавець | Виконавець послуг зі створення КСЗІ ІКС. |
| ДССЗЗІ | Державна служба спеціального зв’язку та захисту інформації. |
| НКЦПФР | Національна комісія з цінних паперів та фондового ринку |
| ДСТУ | Державний стандарт України. |
| Замовник | Державна установа «Агентство з розвитку інфраструктури фондового ринку України» |
| ІКС | Інформаційно-комунікаційна система |
| 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. |
| ОЕ | Об’єкт експертизи. |
| СЗІ | Служба захисту інформації. |
| ТЗ | Технічне завдання. |
| ТЗІ | Технічний захист інформації. |
| ІБД | Інформаційна база даних про ринок цінних паперів та Інформаційна база даних для оприлюднення інформації від імені учасників ринків капіталу та/або професійних організованих товарних ринків; |

*Найменування КСЗІ та її умовне позначення*

*Повне найменування КСЗІ* – комплексна система захисту інформації інформаційно-комунікаційної системи «Комплексна інформаційна система Державної установи «Агентство з розвитку інфраструктури фондового ринку України»

*Скорочена назва* – КСЗІ ІКС «SMIDA+».

Створення комплексної системи захисту інформації для системи: «Інформаційна база даних про ринок цінних паперів та кабінет інформаційних послуг» здійснюється на виконання 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 в сфері технічного захисту інформації інформаційно-комунікаційних систем повинна проводитися у відповідності до вимог Положення про державну експертизу в сфері технічного захисту інформації, затвердженого наказом Адміністрації ДССЗЗІ 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 Держспецзв’язку від 25.03.2011 № 65.

В цьому документі наведені технічні та якісні характеристики, перелік та терміни надання послуг зі створення КСЗІ ІКС. Процес створення КСЗІ ІКС повинен бути побудований у відповідності до вимог національних стандартів України та чинних НД ТЗІ.

**Опис ІКС «SMIDA+».**

Правовою основою діяльності ІКС «SMIDA+» є Закони України «Про інформацію», «Про захист персональних даних», «Про захист інформації в інформаційно-телекомунікаційних системах», «Про електронні довірчі послуги», «Про ринки капіталу та організовані товарні ринки», а також Положення про Державну установу «Агентство з розвитку інфраструктури фондового ринку України», Положення про формування інформаційної бази даних про ринок цінних паперів, затверджене рішенням НКЦПФР від 03.06.2014 № 733 (зі змінами), Порядок подання інформації особами, які провадять діяльність з подання звітності та/або адміністративних даних до Комісії, затверджений рішенням НКЦПФР від 29.11.2018 № 839, інші нормативно-правові акти.

Основними завданнями ІКС «SMIDA+» є:

• автоматизація процесів одержання, збирання, створення, поширення, зберігання і використання інформації для забезпечення функціонування інформаційних баз даних про ринки капіталу та організовані товарні ринки для інформаційного забезпечення діяльності НКЦПФР, учасників ринків капіталу та професійних організованих товарних ринків, інших заінтересованих осіб

• задоволення інформаційних потреб держави, учасників ринків капіталу та професійних організованих товарних ринків, інших заінтересованих осіб про діяльність Національної комісії з цінних паперів та фондового ринку та з питань формування державної політики на ринках капіталу та організованих товарних ринках щодо сприяння розвитку та функціонуванню зазначених ринків на сучасному етапі;

• забезпечення надання інформаційних послуг на ринках капіталу та організованих товарних ринках;

• забезпечення доступу до оприлюдненої інформації від імені учасників ринків капіталу та/або професійних організованих товарних ринків;

• забезпечення процесів подання та обробки звітних даних від суб'єктів подання інформації.

Складовими ІКС «SMIDA+» є:

* основна підсистема;
* резервна підсистема;
* комунікаційна мережа;
* комплексна система захисту інформації.

Основна та резервні підсистеми ІКС «SMIDA+» – сукупність програмно-технічних засобів, призначених для обробки інформації, які забезпечують:

* функціонування ІБД в актуальному стані;
* надання користувачам, відповідно до їх повноважень, доступу до ІБД;
* прийняття та обробку (перевірка, зберігання, та подальша передача її до НКЦПФР або внесення відповідної інформації в ІБД) звітності від суб'єктів подання;
* обмін інформацією між ІКС «SMIDA+», НКЦПФР та суб'єктами подання із використанням засобів криптографічного захисту інформації;
* моніторинг стану інформаційного обміну;
* облік подій в ІКС «SMIDA+», дій користувачів та адміністраторів;
* архівування даних;
* захист інформації під час її обробки.

**1.3. Мета створення КСЗІ ІКС «SMIDA+»**

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 обробки інформації відповідно до чинних нормативно-правових актів України у сфері захисту інформації: Закон України «Про захист інформації в інформаційно-комунікаційних системах», «Про доступ до публічної інформації» та «Про захист персональних даних».

**1.4. Призначення КСЗІ ІКС «SMIDA+»**

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

**1.5. Цілі створення КСЗІ ІКС «SMIDA+»**

Цілі створення КСЗІ ІКС:

* забезпечити максимальний рівень ефективного захисту ІКС;
* забезпечити 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 обробки інформації відповідно до чинних нормативно-правових актів України у сфері захисту інформації;
* забезпечення можливості розвитку захищених систем.

**1.6. Склад послуг зі створення КСЗІ ІКС «SMIDA+»**

Процес створення КСЗІ ІКС повинен бути побудований відповідно до законодавства України, вимог національних стандартів України та чинних НД ТЗІ.

В ході надання послуг з побудови КСЗІ ІКС, у разі необхідності доопрацювання наявної у Замовника документації на ІКС або розширення її комплектності, Виконавець має надати відповідні проекти таких документів.

В межах надання послуг зі створення КСЗІ повинні бути здійснені наступні заходи:

1. Підготовка загальних вимог до КСЗІ ІКС.
2. Розробка та оформлення політик безпеки інформації в ІКС, здійснення вибору основних рішень з протидії всім суттєвим загрозам.
3. Розробка технічних завдань на створення КСЗІ ІКС.
4. Розробка проектів КСЗІ ІКС.
5. Введення КСЗІ ІКС в дію та оцінка захищеності інформації в ІКС.
6. Гарантійне супроводження КСЗІ ІКС.

**2. ВИМОГИ ЧИННОГО ЗАКОНОДАВСТВА**

Надання послуг зі створення КСЗІ повинне відповідати вимогам чинних нормативно правових документів, а саме:

* Закону України «Про інформацію» (із змінами і доповненнями);
* Закону України «Про доступ до публічної інформації»;
* Закону України «Про захист інформації в інформаційно-комунікаційних системах» (із змінами і доповненнями);
* Закон України «Про телекомунікації» (із змінами і доповненнями);
* 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 (із змінами і доповненнями), затвердженій постановою Кабінету Міністрів України від 8 жовтня 1997 року № 1126;
* Положенню про технічний захист інформації в Україні (із змінами і доповненнями), затвердженому постановою Кабінету Міністрів України від 27.09.1999 № 1229;
* Правилам забезпечення захисту інформації в інформаційних, електронних комунікаційних та інформаційно-комунікаційних системах (із змінами і доповненнями), затвердженим постановою Кабінету міністрів України від 29.03.2006 № 373;
* 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 червня 2015 р. № 61 з 2017-07-01;
* 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;
* 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, зареєстрований в Міністерстві юстиції України 10.04.2007 за № 320/13587;
* 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, затверджений наказом ДСТСЗІ СБУ від 28.04.1999 року № 22 (із зміною №1, затвердженому наказом ДСТСЗІ СБУ від 18.06.2002 № 37);
* 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 грудня 2000 року № 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 та керівних документів, що стосуються мети та призначення КСЗІ, повинні бути уточнені при розробці Технічних завдань.

**3. ВИМОГИ ДО СТВОРЕННЯ КСЗІ ІКС «SMIDA+»**

**3.1. Підготовка загальних вимог до КСЗІ**

Підготовка загальних вимог до КСЗІ повинна базуватись на виконанні таких завдань:

* аналіз і визначення наявності у складі інформації, яка підлягає автоматизованій обробці, таких її видів, що потребують обмеження доступу до неї або забезпечення цілісності чи доступності відповідно до вимог нормативно-правових актів;
* обстеження середовища функціонування КСЗІ з аналізом та описом системи, інформаційного та фізичного середовища, а також середовища користувачів з метою підготовки вимог до КСЗІ у вигляді опису кожного середовища функціонування ІКС 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;
* визначення потенційних загроз для інформації;
* розробка моделей загроз;
* формування технічних завдань на створення КСЗІ із урахуванням результатів аналізу ризиків і визначення переліку суттєвих загроз.

**3.2. Розробка та оформлення політик безпеки інформації в КСЗІ, 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».

**3.3. Розробка технічних завдань на створення КСЗІ**

Розробка технічних завдань на створення КСЗІ повинна забезпечувати наступне:

* визначення завдання захисту інформації в ІКС, мета створення КСЗІ, варіант вирішення задач захисту, основні напрями забезпечення захисту;
* здійснення аналізу ризиків (вивчення моделі загроз і моделі порушника, можливих наслідків від реалізації потенційних загроз, величини можливих збитків та ін.) і визначення переліку суттєвих загроз;
* визначення загальних структур та складів КСЗІ, вимоги до можливих заходів, методів та засобів захисту інформації, допустимих обмежень щодо застосування певних заходів і засобів, інших обмежень щодо середовищ функціонування ІКС, обмежень щодо використання ресурсів ІКС для реалізації задач захисту, припустимих витрат на створення КСЗІ, умов створення, введення в дію і функціонування КСЗІ (окремих її підсистем, компонентів), загальних вимог до співвідношення та меж застосування в ІКС (окремих її підсистемах, компонентах) організаційних, інженерно-технічних, технічних, криптографічних та інших заходів захисту інформації, що увійдуть до складу КСЗІ.

**3.4. Розробка проектів КСЗІ**

Розробка проектів КСЗІ повинна забезпечувати виконання наступних завдань:

* розробку техноробочих проектів КСЗІ з відповідним пакетом документації;
* розробку нормативно-розпорядчої документації КСЗІ;
* посадові (функціональні) інструкції співробітників СЗІ, адміністраторів, персоналу та користувачів ІКС;
* технологічні (операційні) інструкції (настанови) щодо виконання завдань з адміністрування та обслуговування КСЗІ (згідно з НД ТЗІ 2.6-001-2011);
* розробку документації щодо проведених випробувань КСЗІ:
* програми та методики випробувань КСЗІ в ІКС;
* проекти протоколів попередніх випробувань КСЗІ в ІКС;
* розробку організаційно-розпорядчої документації КСЗІ:
* проекти актів про прийняття в дослідну експлуатацію КСЗІ ІКС;
* проекти актів завершення дослідної експлуатації КСЗІ ІКС;
* проекти актів завершення робіт зі створення КСЗІ в ІКС;
* розробку супровідної документації КСЗІ:
* формуляри;
* реєстраційні журнали, використовувані для реєстрації фактів та результатів виконання певних завдань з адміністрування та обслуговування КСЗІ.

**3.5. Введення КСЗІ в дію та оцінка захищеності інформації в ІКС**

Введення КСЗІ в дію та оцінка захищеності інформації в ІКС повинні відповідати таким завданням та задовольняти наступним вимогам:

* надання послуг з підготовки організаційних структур та розробки розпорядчих документів, що регламентують діяльність із забезпечення захисту інформації в ІКС;
* проведення попередніх випробувань згідно з програмами та методиками випробувань,
* перевірка працездатності КСЗІ та визначення можливості прийняття їх у дослідну експлуатацію, оформлення протоколів випробувань;
* проведення дослідної експлуатації, під час якої відпрацьовуються технології обробки інформації, обігу машинних носіїв інформації, керування засобами захисту, розмежування доступу користувачів до ресурсів ІКС та автоматизованого контролю за діями користувачів;
* супровід проведення державної експертиз КСЗІ з метою визначення відповідності КСЗІ технічному завданню, вимогам НД із захисту інформації та визначення можливості введення КСЗІ в складі ІКС в експлуатацію;
* усунення недоліків у разі їх виявлення під час проведення державної експертизи.

**3.6. Гарантійне супроводження КСЗІ**

Виконавець впродовж строку дії атестату відповідності КСЗІ зареєстрованого Адміністрацією ДССЗЗІ та експертного висновку до нього, повинен забезпечити гарантійне супроводження КСЗІ ІКС Замовника з дати підписання Акту приймання-передачі наданих послуг, що включає надання інформаційно-консультаційної підтримки щодо експлуатації КСЗІ ІКС Замовника за запитом Замовника.

Допускається виконувати окремі етапи послуг до завершення попередніх етапів, паралельно часі виконання етапів послуг.

**4.1. Склад та зміст етапів надання послуг зі створення КСЗІ ІКС:**

*1й етап*

**Обстеження середовища функціонування ІКС та розробка ТЗ на КСЗІ. Узгодження ТЗ з ДССЗЗІ:**

* *Підготовка організаційно-розпорядчої документації.*

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

За результатами проведеного аналізу Виконавець, спираючись на нормативну базу, що діє в Україні у сфері захисту інформації, готує проекти документів, які визначають організаційну складову КСЗІ (проекти посадових інструкцій і процедур та ін.), які затверджуються Замовником.

* *Обстеження середовищ функціонування ІКС.*

Метою обстеження є підготовка розробником КСЗІ ІКС засадничих даних для формування вимог до КСЗІ у вигляді опису кожного середовища функціонування ІКС 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.

При обстеженні розробником КСЗІ ІКС обчислювальної системи ІКС повинні 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 ін.

Розробником КСЗІ ІКС 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 і характеристики, в тому числі ті, що встановлюються за замовчанням та ін.

Метою такого аналізу є формування розробником КСЗІ в ІКС загального уявлення про наявність потенційних можливостей щодо забезпечення захисту інформації, виявлення компонентів ІКС, які вимагають підвищених вимог до захисту інформації і впровадження додаткових заходів захисту.

При обстеженні розробником КСЗІ ІКС інформаційного середовища, аналізу підлягає вся інформація, що обробляється, а також зберігається в ІКС (дані і програмне забезпечення). Під час аналізу інформація повинна бути класифікована за режимом доступу, за правовим режимом, визначені й описані види її представлення в ІКС.

Для кожного виду інформації і типу об’єкта, в якому вона міститься, ставляться у відповідність властивості захищеності інформації (конфіденційність, цілісність, доступність), яким вони повинні задовольняти.

Аналіз розробником КСЗІ ІКС технології обробки інформації мають бути визначені й описані інформаційні потоки і середовища, через які вони передаються, джерела утворення потоків та 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.

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

При обстеженні фізичного середовища розробником КСЗІ ІКС здійснюється аналіз взаємного розміщення засобів обробки інформації ІКС 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 повинні підлягати такі характеристики фізичного середовища:

- територіальне розміщення компонентів ІКС;

- наявність охорони території та перепускний режим;

- наявність та стан приміщень, в яких мають розміщуватися компоненти ІКС;

- режим доступу до компонентів фізичного середовища ІКС;

- наявність та технічні характеристики систем забезпечення (клімат, живлення, заземлення, тощо);

- наявність проектної та експлуатаційної документації.

При обстеженні розробником КСЗІ ІКС 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 в т.ч. повноважень користувачів щодо управління КСЗІ;

- рівня необхідних прав та можливостей різних категорій користувачів, що повинні мати права доступу до інформації ІКС.

- наявність служби захисту інформації в ІКС.

Результати обстеження середовищ функціонування ІКС повинні бути оформлені розробником КСЗІ ІКС у вигляді акту.

За результатами обстеження середовищ функціонування ІКС розробником КСЗІ ІКС повинен 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.

В разі відсутності служби захисту інформації в ІКС розробляється Положення про Службу захисту інформації.

* *Розробка технічного завдання на створення КСЗІ.*

Фахівці Виконавця розробляють і погоджують із Замовником документ «Технічне завдання на створення КСЗІ», яке визначає всі основні вимоги до КСЗІ і можливі варіанти реалізації її складових елементів. Після узгодження технічного завдання на створення КСЗІ із Замовником, документ узгоджується Виконавцем з ДССЗЗІ. Відповідно до п 5.1 НД ТЗІ 3.7-001- 99 допускається оформлення вимог з захисту інформації у вигляді окремого (часткового) ТЗ, доповнення до загального ТЗ або розділу загального ТЗ.

* *Розробка пакету документів «План захисту інформації».*

Виконавець розробляє частину документації з пакету документів «План захисту інформації»:

* «Модель загроз інформації. Модель порушника».
* «Політика безпеки інформації», які затверджуються Замовником.

***2й етап***

**Проектування КСЗІ ІКС**

* Розробка техноробочого проекту на створення КСЗІ.

Після узгодження технічного завдання на створення КСЗІ з контролюючим органом Виконавець розробляє пакет документів техноробочого проекту на створення КСЗІ.

Техноробочий проект на створення КСЗІ є комплектом документів, в який входить частина документів, розроблених на попередніх етапах, і ряд нових документів, в яких описано, як саме створюватиметься, експлуатуватиметься і, у разі потреби, модернізуватиметься КСЗІ. Техноробочий проект на створення КСЗІ розробляється на підставі і відповідно до технічного завдання на створення КСЗІ. Розробником КСЗІ ІКС повинні виконуватись розроблення, оформлення, узгодження та затвердження документації в обсязі, передбаченому ТЗ на КСЗІ. Зміст та стиль документації повинні бути достатніми для повного опису проектних рішень рівня технічного проекту. Під час розробки проекту КСЗІ обґрунтовуються і приймаються проектні рішення, які дають можливість реалізувати вимоги технічного завдання, забезпечити сумісність і взаємодію різних компонентів КСЗІ, а також різних заходів і способів захисту інформації. В результаті створюється комплект робочої та експлуатаційної документації, необхідної для забезпечення тестування, проведення пусконалагоджувальних робіт, випробувань та управління КСЗІ.

Техноробочий проект на створення КСЗІ включає наступний пакет документів:

* інструкції з експлуатації КСЗІ та її елементів;
* процедури регламентного обслуговування КСЗІ;
* правила і положення по проведенню тестування і аналізу роботи КСЗІ;
* керівництва адміністраторів і користувачів;
* формуляри КСЗІ ІКС.

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

***3й етап***

**Впровадження КСЗІ ІКС**

* *Приведення інформаційної інфраструктури Замовника у відповідність до техноробочого проекту на створення КСЗІ.*

Проводиться виконання робіт з приведення інформаційної інфраструктури замовника у відповідність до техноробочого проекту на створення КСЗІ.

В разі відсутності у Замовника СЗІ, вона повинна створена(призначення відповідальних осіб за захист інформації) – затверджено «Положення про Службу захисту інформації». Розробником КСЗІ ІКС має бути завершена розробка, а також подані Замовнику на затвердження документи, що входять до плану захисту (за виключенням тих, для розробки яких необхідні результати наступних етапів послуг).

Розробка плану захисту повинна бути здійснена розробником КСЗІ ІКС згідно з НД ТЗІ 1.4-001.

* *Проведення пусконалагоджувальних робіт та навчання користувачів.*

Виконавець проводить всі пусконалагоджувальні роботи, навчання та інструктажі персоналу Замовника згідно з правилами і режимами експлуатації КСЗІ.

Проводяться наступні заходи:

* організація захисту інформації від несанкціонованого доступу (НСД);
* організація антивірусного захисту інформації;
* розробка програми і методики проведення попередніх випробувань;
* проведення попередніх випробувань.
* *Випробування КСЗІ.*

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

Попередні випробування повинні бути проведені розробником КСЗІ ІКС згідно з Програмою та методиками проведення попередніх випробувань. Програму й методику проведення попередніх випробувань готує розробник КСЗІ, а погоджує замовник КСЗІ ІКС.

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

- *Проводиться дослідна експлуатація, під час якої:*

* відпрацьовуються технології обробки інформації, облік машинних носіїв інформації, управління засобами захисту, розмежування доступу користувачів до ресурсів ІКС і автоматизованого контролю за діями користувачів;
* співробітники служби захисту інформації і користувачі ІКС набувають практичних навичок з використання технічних і програмно-апаратних засобів захисту інформації, засвоюють вимоги організаційних і розпорядчих документів з питань розмежування доступу до технічних засобів і інформаційних ресурсів;
* здійснюється (за необхідністю) доопрацювання програмного забезпечення, додаткове налагодження та конфігурування КЗЗ;
* здійснюється (за необхідністю) коригування робочої та експлуатаційної документації. За результатами дослідної експлуатації приймається рішення щодо готовності КСЗІ ІКС до подання на державну експертизу.

***4й етап***

**Супровід проведення державної експертизи КСЗІ ІКС і отримання «Атестата відповідності»**

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

* підготовки КСЗІ до проведення державної експертизи в ДССЗЗІ і супроводі експертних випробувань;
* узгодження з ДССЗЗІ результатів експертизи і забезпечення видачі й передачі Замовнику Атестата відповідності.

Державна експертиза проводиться з метою визначення відповідності КСЗІ технічному завданню на створення КСЗІ, вимогам нормативної документації із захисту інформації і визначення можливості введення КСЗІ ІКС в експлуатацію.

Під час виконання заходів щодо проведення додаткових державних експертиз Виконавець здійснює попередній аналіз ОЕ та документації КСЗІ ІКС з метою визначення наявності або відсутності змін у середовищах функціонування ІКС або змін у реалізації ОЕ порівняно з тими, які досліджувалися та оцінювалися при проведенні первинної експертизи. Якщо за результатами аналізу встановлено, що у середовищах функціонування ІКС або реалізації ОЕ відбулися зміни, тобто середовища функціонування ІКС або певні структурні компоненти ОЕ не відповідають тим, стосовно яких здійснювалися експертні роботи при проведенні попередньої експертизи, Виконавець здійснює доопрацювання документації КСЗІ на ІКС та/або розширення її комплектності, та розробляє нові програми та методики проведення експертизи (у разі необхідності). Після внесення змін до документації КСЗІ або в разі їх відсутності, Виконавець здійснює підготовку КСЗІ до проведення державної експертизи в ДССЗЗІ і супровід експертних випробувань з подальшим узгодженням з ДССЗЗІ результатів експертизи і забезпеченням видачі й передачі Замовнику Атестата відповідності.

У разі виявлення недоліків під час проведення державної експертизи, їх усунення здійснюється до завершення державної експертизи, порядок усунення такий самий, як і для попередніх випробувань згідно з НД ТЗІ 3.7-003 -2005. Якщо в силу якихось причин усунути недоліки в ході експертизи неможливо, це оформлюється актом, до якого вноситься перелік необхідних доробок та рекомендації щодо їх виконання. Після завершення передбачених актом робіт проводиться повторна експертиза.

В рамках заходів з організації та проведення державних експертиз КСЗІ ІКС, в тому числі додаткових, Виконавець повинен забезпечити надання наступних послуг:

* попередній аналіз стану забезпечення захисту ІКС та реалізованих організаційно технічних та організаційних заходів;
* за необхідності вносяться зміни до матеріалів ОЕ, актуалізація стану, підготовка додаткової інформації щодо ОЕ, коригування впроваджених організаційно-технічних заходів відповідно до зауважень, рекомендацій експерта;
* результати проведення експертних випробувань КСЗІ ІКС повинні бути оформлені відповідними протоколами та проектом експертного висновку на КСЗІ ІКС, який узгоджується з Держспецзв’язку.

|  |  |
| --- | --- |
| **ЗАМОВНИК** | **ВИКОНАВЕЦЬ** |
| **Державна установа «Агентство з розвитку інфраструктури фондового ринку України»** |  |
| **\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_**  **м. п.** | **\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_**  **м. п.** |