**Додаток 2 до тендерної документації**

**(Інформація про необхідні технічні, якісні та кількісні характеристики**

**предмету закупівлі – технічна специфікація)**

Послуги зі створення комплексної системи захисту інформації в інформаційно-комунікаційній системі «Медична інформаційна система Комунального некомерційного підприємства Харківської обласної ради "Центр екстреної медичної допомоги та медицини катастроф" (із комплектуванням засобами криптографічного захисту інформації) та забезпечення проведення її державної експертизи

ДК 021:2015:72220000-3: “Консультаційні послуги з питань систем та з технічних питань”

**Розділ І. Опис предмету закупівлі:**

* 1. Кількість та загальні характеристики предмету закупівлі наведені у Таблиці 1.

*Таблиця 1*

|  |  |  |
| --- | --- | --- |
| **Найменування:** | **Кількість** | **Одиниця**  **виміру** |
| Послуги зі створення комплексної системи захисту інформації в інформаційно-комунікаційній системі «Медична інформаційна система Комунального некомерційного підприємства Харківської обласної ради "Центр екстреної медичної допомоги та медицини катастроф" (із комплектуванням засобами криптографічного захисту інформації) та забезпечення проведення її державної експертизи | 1 | послуга |

**Розділ ІІ Призначення комплексної системи захисту інформації та відповідність її положенням нормативно-правових актів**

2.1. Для захисту інформації в інформаційно-комунікаційній системі «Медична інформаційна система Комунального некомерційного підприємства Харківської обласної ради "Центр екстреної медичної допомоги та медицини катастроф" Виконавцем мають бути надані послуги зі створення комплексної системи захисту інформації (КСЗІ) та забезпечено проведення її державної експертизи. КСЗІ має забезпечувати захист інформації від несанкціонованих дій з інформацією.

2.2. Послуги з створення КСЗІ в інформаційно-комунікаційній системі «Медична інформаційна система Комунального некомерційного підприємства Харківської обласної ради "Центр екстреної медичної допомоги та медицини катастроф" повинні бути надані у обсязі, передбаченому НД ТЗІ 3.7-003-05 «Порядок проведення робіт із створення комплексної системи захисту інформації в інформаційно-телекомунікаційній системі».

2.3. Відповідність КСЗІ вимогам нормативно-правових актів та нормативних документів з питань ТЗІ має бути підтверджена за результатами державної експертизи КСЗІ, що проводиться згідно з Положенням про державну експертизу у сфері ТЗІ, затвердженим наказом Адміністрації Держспецзв’язку від 16.05.2007 № 93, зареєстрованим в Міністерстві юстиції України 16.07.2007 за № 820/14087 (із змінами, внесеними згідно з Наказом Адміністрації Державної служби спеціального зв'язку та захисту інформації № 567 від 10.10.2012).

2.4. Виконавець на безоплатній основі здійснює супроводження державної експертизи КСЗІ в інформаційно-комунікаційній системі «Медична інформаційна система Комунального некомерційного підприємства Харківської обласної ради "Центр екстреної медичної допомоги та медицини катастроф", в тому числі оплачує вартість її проведення. У разі отримання під час експертизи зауважень та пропозицій до КСЗІ, Виконавець здійснює їх усунення на безоплатній основі у терміни, узгоджені з Замовником.

2.5. КЗСІ має відповідати положенням наступних нормативно-правових актів:

*Положення про технічний захист інформації в Україні*. Затверджено Указом Президента України від 27.09.99 № 1229.

*Правила забезпечення захисту інформації в* *інформаційних, електронних комунікаційних та інформаційно-комунікаційних системах*. Затверджені постановою Кабінету Міністрів України від 29.03.2006 № 373.

ДСТУ 3396.1-96 Захист інформації. Технічний захист інформації. Порядок проведення робіт.

ДСТУ 3396.2-97 Захист інформації. Технічний захист інформації. Терміни і визначення.

*Положення про державну експертизу в сфері технічного захисту інформації*. Затверджено наказом Адміністрації Державної служби спеціального зв'язку та захисту інформації України від 16.05.2007 № 93. Зареєстровано в Міністерстві юстиції України 16.07.2007 за № 820/14087.

*Положення про порядок розроблення, виробництва та експлуатації засобів криптографічного захисту конфіденційної інформації та відкритої інформації з використанням електронного цифрового підпису*. Затверджено наказом Адміністрації Державної служби спеціального зв'язку та захисту інформації України від 20.07.2007 № 141. Зареєстровано в Міністерстві юстиції України 30.07.2007 за № 862/14129.

НД ТЗІ 1.1-002-99 Загальні положення щодо захисту інформації в комп'ютерних системах від несанкціонованого доступу.

НД ТЗІ 1.4-001-2000 Типове положення про службу захисту інформації в автоматизованій системі.

НД ТЗІ 1.6-003-04 Створення комплексів технічного захисту інформації на об’єктах інформаційної діяльності. Правила розроблення, побудови, викладення та оформлення моделі загроз для інформації.

НД ТЗІ 2.5-004-99 Критерії оцінки захищеності інформації в комп'ютерних системах від несанкціонованого доступу.

НД ТЗІ 2.5-005-99 Класифікація автоматизованих систем і стандартні функціональні профілі захищеності оброблюваної інформації від несанкціонованого доступу.

НД ТЗІ 2.5-007-2007 Вимоги до комплексу засобів захисту інформації, що становить державну таємницю, від несанкціонованого доступу при її обробленні в автоматизованих системах класу "1".

НД ТЗІ 2.5-008-02 Вимоги із захисту конфіденційної інформації від несанкціонованого доступу під час оброблення в автоматизованих системах класу 2.

НД ТЗІ 2.5-010-03 Вимоги до захисту інформації WEB-сторінки від несанкціонованого доступу.

НД ТЗІ 2.7-009-09 Методичні вказівки з оцінювання функціональних послуг безпеки в засобах захисту інформації від несанкціонованого доступу.

НД ТЗІ 2.7-010-09 Методичні вказівки з оцінювання рівня гарантій коректності реалізації функціональних послуг безпеки в засобах захисту інформації від несанкціонованого доступу.

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.

НД ТЗІ 3.7-001-99 Методичні вказівки щодо розробки технічного завдання на створення комплексної системи захисту інформації в автоматизованій системі.

НД ТЗІ 3.7-003-05 Порядок проведення робіт із створення комплексної системи захисту інформації в інформаційно-телекомунікаційній системі.

ДЕРЖСТАНДАРТ 34.201–89 Інформаційна технологія. Комплекс стандартів на автоматизовані системи. Види, комплектність та позначення документів при створенні автоматизованих систем.

ДЕРЖСТАНДАРТ 34.602 Інформаційна технологія. Комплекс стандартів на автоматизовані системи. Технічне завдання створення автоматизованої системи.

РД 50-34.698-90 Методичні вказівки. Інформаційна технологія. Комплекс стандартів та керівних документів на автоматизовані системи. Вимоги щодо змісту документів.

**Розділ ІІІ. Етапи створення КСЗІ (перелік необхідних заходів)**

*Таблиця 2*

|  |  |  |
| --- | --- | --- |
| № **з/п** | **Найменування** | **Результат** |
| **Створення комплексної системи захисту інформації** | | |
| 1. | Формування загальних вимог до КСЗІ ІКС  Розробка політики безпеки інформації | 1) Акт обстеження середовищ функціонування.  2) Проект акту категорування об’єкту інформаційної діяльності (за потреби).  3) Опис моделі загроз інформації.  4) Опис моделі порушника безпеки інформації.  5) Опис політики безпеки інформації. |
| 2. | Розробка технічного завдання на КСЗІ ІКС | Розроблене Технічне завдання на створення КСЗІ ІКС. |
| 3. | Постачання та налаштування засобу криптографічного захисту інформації, які входять до складу КЗЗ КСЗІ ІКС | Наданий та налаштований засіб криптографічного захисту інформації. |
| 4. | Розробка техноробочого проекту | Матеріали техноробочого проекту |
| 5. | Підготовка КСЗІ ІКС до введення в дію, пусконалагоджувальні роботи | 1) Положення про службу захисту інформації.  2) План захисту інформації.  3) Проект наказу про створення СЗІ та призначення відповідальних осіб.  4) Проект наказу про створення комісії та проведення попередніх випробувань та дослідної експлуатації |
| 6. | Попередні випробування КСЗІ ІКС | 1) Програма та методика попередніх випробувань.  2) Протокол попередніх випробувань. |
| 7. | Дослідна експлуатація КСЗІ ІКС | 1) Акт приймання КСЗІ ІКС у дослідну експлуатацію. 2) Акт завершення дослідної експлуатації КСЗІ ІКС.  3) Акт завершення робіт зі створення КСЗІ ІКС.  4) Формуляр. |
| **Організація проведення первинної державної експертизи комплексної системи захисту інформації** | | |
| 1. | Подача заявки до Адміністрації Держспецзв’язку на проведення державної експертизи КСЗІ ІКС | Проект Заявки на проведення державної експертизи КСЗІ ІКС |
| 2. | Забезпечення розроблення програми та методики експертизи КСЗІ ІКС Організатором | Програма та методика державної експертизи КСЗІ ІКС  (Замовнику не надаються. Програма погоджується Замовником) |
| 3. | Забезпечення проведення експертних випробувань та досліджень ОЕ за розробленими програмою та методикою експертизи КСЗІ ІКС Організатором | Протокол виконання робіт з експертизи КСЗІ ІКС  (Замовнику не надається) |
| 4. | Забезпечення оформлення результатів експертизи та підготовка експертного висновку Організатором | Проект Експертного висновку на КСЗІ ІКС |

Час супроводження процесу опрацювання в Адміністрації Держспецзв’язку результатів експертизи та оформлення для Замовника Атестата відповідності КСЗІ ІКС вимогам нормативних документів з технічного захисту інформації Організатором, не входить до вказаного в Договорі строку надання послуг. Атестат відповідності та Експертний висновок надається Замовнику після реєстрації Адміністрацією Держспецзв’язку.

**Розділ IV Вимоги до складу заходів**

4.1 На *етапі формування загальних вимог до КСЗІ в ІКС* повинні бути виконані наступні заходи:

4.1.1 Обґрунтування необхідності створення КСЗІ:

4.1.1.1 Підставою для визначення необхідності створення КСЗІ є норми та вимоги законодавства України, які встановлюють обов’язковість обмеження доступу до певних видів інформації або забезпечення її цілісності чи доступності, або прийняте власником інформації рішення щодо цього, якщо нормативно-правові акти надають йому право діяти на власний розсуд.

4.1.1.2 Вихідні дані для обґрунтування необхідності створення КСЗІ повинні бути отримані за результатами:

- аналізу нормативно-правових актів (державних, відомчих та таких, що діють в межах установи, організації, підприємства), на підставі яких може встановлюватися обмеження доступу до певних видів інформації чи заборона такого обмеження, або визначатися необхідність забезпечення захисту інформації згідно з іншими критеріями;

- 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;

- оцінки можливих переваг (фінансово-економічних, соціальних і т.п.) експлуатації ІКС у разі створення КСЗІ.

4.1.1.3 На підставі проведеного аналізу повинно бути обґрунтовано рішення про необхідність створення КСЗІ.

4.1.2 Обстеження середовищ функціонування ІКС:

4.1.2.1 Під час виконання цих робіт ІКС розглядається як організаційно-технічна система, яка поєднує обчислювальну систему, фізичне середовище, середовище користувачів, оброблювану інформацію і технологію її обробки (далі - середовища функціонування ІКС).

4.1.2.2 Метою обстеження є підготовка 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 робіт.

4.1.2.3 При обстеженні обчислювальної системи ІКС повинні бути 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.

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 умовчанням та ін.

Метою такого аналізу є надання 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.

4.1.2.4 При обстеженні 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) чи ІКС (спостережність), яким вони повинні задовольняти.

Аналіз технології обробки інформації повинен виявити особливості обігу електронних документів, 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 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.

4.1.2.5 При обстеженні фізичного середовища 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 (генеральний план, ситуаційний план);

- наявність охорони території та перепускний режим;

- наявність категорійованих приміщень, в яких мають розміщуватися компоненти ІКС;

- режим доступу до компонентів фізичного середовища ІКС;

- наявність та технічні характеристики систем заземлення;

- умови зберігання магнітних, оптико-магнітних, паперових та інших носіїв інформації;

- наявність проектної та експлуатаційної документації на компоненти фізичного середовища.

4.1.2.6 При обстеженні середовища користувачів здійснюється аналіз:

- функціонального та кількісного складу користувачів, їхніх функціональних обов’язків та рівня кваліфікації;

- повноважень користувачів щодо допуску до відомостей, які обробляються в ІКС, доступу до ІКС та її окремих компонентів;

- повноважень користувачів щодо управління КСЗІ;

- рівня можливостей різних категорій користувачів, що надаються (можуть бути доступними) їм засобами ІКС.

- наявності служби захисту інформації в ІКС.

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

4.1.2.8 За результатами обстеження середовищ функціонування 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.

4.2 На етапі *розробки політики безпеки інформації в ІКС* повинна бути виконана розробка та оформлення **Політики безпеки інформації в ІКС**.

4.2.1 На цьому етапі повинно бути здійснено:

- вибір основних рішень з протидії всім суттєвим загрозам, формування загальних вимог, правил, обмежень, рекомендацій і т.п., які регламентують використання захищених технологій обробки інформації в ІКС, окремих заходів і засобів захисту інформації, діяльність користувачів всіх категорій;

- документальне оформлення політики безпеки інформації.

4.2.2 Політика безпеки може розроблятись для ІКС в цілому або, якщо мають місце особливості функціонування окремих компонентів КСЗІ, для окремої компоненти, для окремої функціональної задачі, для окремої технології обробки інформації тощо.

4.2.3 Політика безпеки повинна розроблятись згідно з положеннями НД ТЗІ 1.1-002 та рекомендаціями НД ТЗІ 1.4-001.

4.3 На етапі *розробки технічного завдання на створення КСЗІ* повинна бути виконана розробка **Технічного завдання** **на створення КСЗІ в ІКС**:

4.3.1 **ТЗ на створення КСЗІ в ІКС** є засадним організаційно-технічним документом, який визначає вимоги із захисту оброблюваної в ІКС інформації, порядок створення КСЗІ, порядок проведення всіх видів випробувань КСЗІ та введення її в експлуатацію в складі ІКС.

4.3.2 **ТЗ на створення КСЗІ** повинно розроблятись з урахуванням комплексного підходу до побудови КСЗІ, який передбачає об'єднання в єдину систему усіх необхідних заходів і засобів захисту від різноманітних загроз безпеці інформації на всіх етапах життєвого циклу ІКС.

4.3.3 Розроблення та оформлення ТЗ на КСЗІ його зміст, порядок погодження та затвердження повинен відповідати НД ТЗІ 3.7-001 та ГОСТ 34.602.

4.4 На етапі *розробки проекту КСЗІ* повинні бути виконані наступні заходи:

4.4.1 Порядок розробки проекту КСЗІ:

4.4.1.1 Проект КСЗІ повинен бути розроблений на підставі та у відповідності до ТЗ на створення ІКС.

4.4.1.2 Під час розробки проекту КСЗІ повинні бути обґрунтовані і прийняті проектні рішення, які дають змогу реалізувати вимоги ТЗ, забезпечити сумісність і взаємодію різних компонентів КСЗІ, а також різних заходів і способів захисту інформації.

4.4.1.3 Для всіх стадій розробки проекту КСЗІ склад документації визначається ТЗ на КСЗІ, види та зміст – ГОСТ 34.201, НД ТЗІ 2.5-004. Документація на програмні засоби виконується згідно з комплексом стандартів ЄСПД, на технічні засоби – згідно з комплексом стандартів ЄСКД.

4.4.2 Ескізний проект КСЗІ:

4.4.2.1 На цьому етапі повинна бути здійснена розробка попередніх проектних рішень КСЗІ та, у разі необхідності, її окремих складових частин, а також розроблення, оформлення, узгодження та затвердження документації на КСЗІ. Зміст та стиль документації повинні бути достатніми для повного опису проектних рішень рівня ескізного проекту.

4.4.2.2 Повинні бути визначені: функції КСЗІ в цілому та функції її окремих складових частин; склад організаційних, правових та інших заходів захисту; склад комплексу засобів захисту інформації від несанкціонованого доступу (далі – КЗЗ); узагальнена структура КСЗІ та схема взаємодії складових частин.

4.4.2.3 Повинні бути запропоновані попередні технічні рішення, за допомогою яких передбачається реалізація завдань і функцій КСЗІ.

4.4.3 Технічний проект КСЗІ

4.4.3.1 Розробка проектних рішень КСЗІ

Повинна бути виконана розробка: загальних проектних рішень, необхідних для реалізації вимог ТЗ на КСЗІ; рішень щодо структури КСЗІ (організаційної структури, технічних і програмних засобів), алгоритмів функціонування та умов використання засобів захисту; рішень щодо архітектури КЗЗ та механізмів реалізації, визначених функціональним профілем послуг безпеки інформації.

Повинні бути здійснені організаційно-технічні заходи щодо забезпечення послідовності розробки КЗЗ, архітектури, середовища розробки, випробувань, середовища функціонування та експлуатаційної документації КЗЗ у відповідності до заданих рівнем гарантій реалізації послуг безпеки згідно із специфікаціями НД ТЗІ 2.5-004, НД ТЗІ 2.5-007, НД ТЗІ 2.5-008, НД ТЗІ 2.5-010.

4.4.3.2 Розробка документації на КСЗІ

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.

4.4.3.3 Розробка документації на постачання засобів захисту інформації та/або технічних вимог (технічних завдань) на їх розробку.

Повинні бути підготовлена та оформлена документація на постачання засобів захисту або продукції, що містить їх у своєму складі, для комплектації КСЗІ. Якщо необхідної продукції немає на ринку засобів захисту, то визначаються технічні вимоги (складаються технічні завдання) на розроблення відповідних засобів.

4.4.3.4 Розробка завдань на проектування в суміжних частинах повинно здійснюватися розроблення, оформлення і затвердження завдань на проектування з суміжних питань, які пов’язані зі створенням КСЗІ або впливають на умови її функціонування (будівельні, електротехнічні, санітарно-технічні та інші підготовчі роботи).

4.4.4 Робочий проект КСЗІ

4.4.4.1 На цьому етапі повинно бути здійснено розроблення, оформлення та затвердження робочої та експлуатаційної документації КСЗІ та, у разі необхідності, її окремих складових частин.

Робоча документація повинна містити детальні рішення щодо реалізації технічного проекту КСЗІ, щодо забезпечення управління КСЗІ і взаємодії її компонентів, а також документацію, необхідну для тестування, проведення пусконалагоджувальних робіт, проведення випробувань КСЗІ.

4.4.4.2 Повинна проводитись розробка засобів захисту інформації, передбачених п. 4.4.3.3 Технічних вимог, або адаптація готової продукції до умов функціонування КСЗІ. Розробка засобів захисту інформації від НСД повинна здійснюватися здійснюється згідно з НД ТЗІ 3.6-001.

4.4.4.3 До складу робочої документації на КЗЗ повинні входити описи процедур інсталяції та ініціалізації комплексу, налагодження всіх механізмів розмежування доступу користувачів до інформації та апаратних ресурсів ІКС, контролю за діями користувачів, формування та актуалізації баз даних захисту, а також контролю цілісності програмного забезпечення та баз даних захисту.

Документація робочого проекту повинна містити вихідні дані для внесення їх до баз даних захисту.

4.4.4.5 Експлуатаційна документація повинна включати опис порядку функціонування КСЗІ та настанови (інструкції) щодо забезпечення цього порядку обслуговуючим персоналом і користувачами, порядку супроводження КСЗІ впродовж життєвого циклу ІКС.

Дозволяється вилучати етап «Ескізний проект КСЗІ», а також поєднувати етапи «Технічний проект КСЗІ» і «Робочий проект КСЗІ» в один етап «Техноробочий проект КСЗІ».

4.5 На етапі *введення КСЗІ в дію та оцінки захищеності інформації в ІКС* повинні бути виконані наступні заходи:

4.5.1 Підготовка КСЗІ до введення в дію

4.5.1.1 Повинні бути проведені роботи з підготовки організаційної структури та розробки розпорядчих документів, що регламентують діяльність із забезпечення захисту інформації в ІКС.

4.5.1.2 Повинно бути здійснено створення СЗІ (призначення відповідальних осіб за захист інформації).

4.5.1.3 В основному має бути завершена розробка і затверджені документи, що входять до плану захисту (за виключенням тих, для розробки яких необхідні результати наступних етапів робіт).

4.5.1.4 Створення СЗІ та розробка плану захисту повинні бути здійснені згідно з НД ТЗІ 1.4-001.

4.5.2 Навчання користувачів

Повинно бути проведено навчання користувачів ІКС всіх категорій (технічного обслуговуючого персоналу, звичайних користувачів та користувачів, які мають повноваження щодо управління засобами КСЗІ та ін.) в частині, що їх стосується, основним положенням документів плану захисту, які необхідні їм для дотримання правил політики безпеки інформації, експлуатації засобів захисту інформації тощо, перевірка їх уміння користуватись впровадженими технологіями захисту інформації і реєстрація результатів навчання.

4.5.3 Комплектування КСЗІ

Повинно бути забезпечено отримання продукції (засобів захисту інформації, матеріалів, обладнання та ін.) від постачальників та співвиконавців робіт. Приймається рішення щодо підготовки до проведення оцінки на відповідність вимогам НД ТЗІ засобів захисту, які на момент проектування КСЗІ не мали відповідних сертифікатів або експертного висновку, а також порядку проведення такої оцінки під час державної експертизи КСЗІ.

4.5.4 Пусконалагоджувальні роботи

4.5.4.1 Метою пусконалагоджувальних робіт є:

- встановлення і налагодження КЗЗ;

- перевірка працездатності засобів захисту інформації в автономному режимі та при їх комплексній взаємодії.

4.5.4.2 Повинні бути здійснені згідно з документацією робочого проекту інсталяція, ініціалізація та перевірка працездатності КЗЗ.

Інсталяція та ініціалізація КЗЗ, який має експертний висновок щодо його відповідності вимогам НД ТЗІ, повинна здійснюватися у порядку, визначеному в експлуатаційній документації на лекс.

Під час інсталяції мають бути задіяні всі механізми розмежування доступу користувачів до інформації та апаратних ресурсів ІКС, контролю за діями користувачів, а також контролю цілісності програмного забезпечення та бази даних захисту КЗЗ.

До бази даних захисту повинні бути внесені відомості про користувачів ІКС, встановлюються їх повноваження щодо доступу до захищених об’єктів КС, їх створення, модифікації, архівування, знищення, експорту/імпорту із системи та інші дані.

4.5.5 Попередні випробування

4.5.5.1 Метою попередніх випробувань є перевірка працездатності КСЗІ та визначення можливості прийняття її у дослідну експлуатацію.

Під час випробувань перевіряються працездатність КСЗІ та відповідність її вимогам ТЗ.

4.5.5.2 Попередні випробування повинні бути проведені згідно з Програмою та методиками випробувань. Програма та методики випробувань, протоколи випробувань розробляються та оформлюються згідно з вимогами РД 50-34.698.

4.5.5.3 Попередні випробування організовує замовник ІКС, а проводить розробник КСЗІ спільно із замовником. Для проведення попередніх випробувань замовником ІКС створюється комісія. Головою комісії призначається представник замовника.

4.5.5.4 Результати попередніх випробувань оформлюються протоколом випробувань, де міститься висновок щодо можливості прийняття КСЗІ у дослідну експлуатацію, а також перелік виявлених недоліків, необхідних заходів з їх усунення, і рекомендовані терміни виконання цих робіт.

4.5.5.5 Після усунення недоліків у випадку їх наявності та коригування проектної, робочої, експлуатаційної документації КСЗІ оформлюється Акт про приймання КСЗІ у дослідну експлуатацію.

4.5.6 Дослідна експлуатація

4.5.6.1 Під час дослідної експлуатації КСЗІ:

повинні бути відпрацьовані технології оброблення інформації, обігу машинних носіїв інформації, керування засобами захисту, розмежування доступу користувачів до ресурсів ІКС та автоматизованого контролю за діями користувачів;

співробітники СЗІ та користувачі ІКС повинні набути практичних навичок з використання технічних та програмно-апаратних засобів захисту інформації, засвоїти вимоги організаційних та розпорядчих документів з питань розмежування доступу до технічних засобів та інформаційних ресурсів;

здійснено додаткове налагоджування та конфігурування КЗЗ;

здійснено (за необхідністю) коригування робочої та експлуатаційної документації.

За результатами робіт за довільною формою повинен бути складений акт про завершення дослідної експлуатації, який містить висновок щодо можливості (неможливості) представлення КСЗІ на державну експертизу.

4.5.7 Державна експертиза КСЗІ

4.5.7.1 Державна експертиза проводиться з метою визначення відповідності КСЗІ технічному завданню, вимогам НД із захисту інформації та визначення можливості введення КСЗІ в складі ІКС в експлуатацію.

Державна експертиза КСЗІ в ІКС проводиться згідно з *Положенням про державну експертизу в сфері технічного захисту інформації*.

4.5.7.2 Виявлені під час державної експертизи недоліки усуваються до її завершення, порядок усунення такий самий, як і для попередніх випробувань. 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.

4.5.7.3 Допускається розпочинати і проводити державну експертизу КСЗІ паралельно з роботами етапів проектування.

**Розділ V Постачання засобу криптографічного захисту інформації**

Необхідно передбачити постачання засобу криптографічного захисту інформації для забезпечення захищеного обміну даними між віддаленими робочими місцями користувачів ІКС та серверною частиною ІКС (вимоги визначені в таблиці 3).

*Таблиця 3*

| **№ з/п** | **Вимоги до засобу криптографічного захисту інформації** | **Деталізація вимог** |
| --- | --- | --- |
| 1.1 | Реалізація шлюзів у вигляді образу віртуальної машини (virtual appliance) з попередньо налаштованими операційною системною та програмним забезпеченням у віртуальній інфраструктурі основного ЦОД | Постачання у вигляді Virtual Appliance для середовищ віртуалізації VMware тощо |
| 1.2 | Завдання на захист процедури реєстрації, автентифікації і т.д. покладається на проксі-сервери, для побудови HTTPS з’єднання | Обов’язково з використанням TLS v1.2+ |
| 1.3 | Можливість горизонтального масштабування пропускної здатності за рахунок збільшення кількості серверів (virtual appliance). | Без обмежень на кількість |
| 1.4 | Забезпечення пропускної здатності захищеного каналу між користувачами та (за умови наявності якісного Інтернет з’єднання між користувачем і проксі-сервером) | Не менше 100 Мбіт/с |
| 1.5 | Можливість роботи через HTTP-proxy | Обов’язково |
| 1.6 | Засіб КЗІ, який використовується для побудови TLS v1.2 на боці проксі-сервера повинен мати відповідний діючий позитивний експертний висновок Держспецзв’язку України. | Обов’язково |
| 1.7 | Кількість Virtual Appliance з засобом КЗІ | 1 шт. з можливістю масштабування |
| 1.8 | Кількість комплектів, які прив’язані до відповідного ЦОД | 1 шт. в ЦОД |
| 1.9 | Кількість користувачів, які підключаються до проксі-сервера | Без обмеження кількості |

Учасник повинен у складі пропозиції надати:

1. На підтвердження наявності ліцензії на провадження господарської діяльності з надання послуг у галузі криптографічного захисту інформації (крім послуг електронного цифрового підпису) та технічного захисту інформації Учасник має надати копії ліцензії на провадження господарської діяльності з надання послуг у галузі криптографічного захисту інформації (крім послуг електронного цифрового підпису) та технічного захисту інформації, за переліком, що визначається Кабінетом Міністрів України, у разі відсутності інформації про учасника в переліку суб’єктів господарювання, що мають ліцензії на провадження господарської діяльності з надання послуг у галузі криптографічного захисту інформації (крім послуг електронного цифрового підпису) та технічного захисту інформації, за переліком, що визначається Кабінетом Міністрів України, який розміщено на офіційному веб-сайті Державної служби спеціального зв'язку та захисту інформації України у розділі: Про Держспецзв’язку/Послуги Держспецзв’язку/ Ліцензування/ Перелік суб’єктів господарювання, що мають ліцензії на провадження господарської діяльності з надання послуг у галузі криптографічного захисту інформації (крім послуг електронного цифрового підпису) та технічного захисту інформації, за переліком, що визначається Кабінетом Міністрів України/Ліцензіати.

2. Копію авторизаційного листа від розробника (виробника) засобу криптографічного захисту інформації для даної закупівлі, який підтверджує повноваження учасника від розробника (виробника) засобу криптографічного захисту інформації на постачання необхідного засобу криптографічного захисту інформації (у разі якщо Учасник не є розробником (виробником) запропонованого засобу криптографічного захисту інформації).

3. Копію діючого експертного висновку на засіб криптографічного захисту інформації, який пропонується учасником.