ЗАТВЕРДЖЕНО

Рішення Комісії з відбору консультантів,
товарів, робіт та неконсультаційних послуг
спільних зі Світовим банком проєктів
протокол засідання № 339 від 06.10.2023

**Міністерство охорони здоров'я України**
Проект № 9468-UA
«Зміцнення системи охорони здоров'я та збереження життя в Україні» (HEAL Ukraine)

# ЗАПИТ ДО ПОДАННЯ ЦІНОВИХ ПРОПОЗИЦІЙ
## за пакетом № HEAL-RFQ-4.1.1.9
## «Забезпечення функціонування Галузевого центру кібербезпеки сфери охорони здоров'я»

1. Україна одержала позику Міжнародного банку реконструкції та розвитку (далі - Банк) 9468-UA на фінансування проекту «Зміцнення системи охорони здоров'я та збереження життя» (HEAL Ukraine) (далі - Проєкт). Частина коштів цієї Позики має бути використана для покриття витрат в рамках договору, до якого відноситься цей запит до подання цінових пропозицій (далі – Запит).

2. Міністерство охорони здоров'я України (далі – Покупець) цим листом запрошує правомочних учасників торгів (тобто учасників, товари та/або програмне забезпечення, які вони пропонують, не підпадають під обмежувальні заходи (санкції) введені відповідно до чинних Указів Президента України) надіслати цінові пропозиції щодо н з постачання Програмної продукції та супровідних послуг для забезпечення функціонування Галузевого центру кібербезпеки сфери охорони здоров'я:

   - Підсистема управління подіями інформаційної безпеки (SIEM+SOAR) на 5000 EPS – 1 комплект;
   - Підсистема аудиту дій користувачів та надання доступу до критично важливих систем – 1 комплект;
   - Підсистема для фільтрації мережевого трафіку та захисту мережі, аналізу запобігання мережевих вторгнень – 2 комплекти;
   - Підсистема для забезпечення захисту веб-додатків - 1 комплект;
   - Послуги зі встановлення, налаштування та інтеграції вказаних комплектів програмної продукції;
   - Навчання персоналу Покупця.

   Інформація щодо Технічних вимог та обсягів виконання вказана в Додатках.

3. Учасник подає лише одну цінову пропозицію. Всі пропозиції учасника, який надав більше одної цінової пропозиції, будуть відхилені. Пропозиції мають бути повними (включати усі позиції) відповідно до цього Запиту. Неповні пропозиції будуть відхилені. Цінові пропозиції оцінюватимуться за всіма позиціями та договір буде присуджено фірмі, яка запропонувала найменшу оцінену вартість всіх позицій та відповідає усім умовам, встановленим цим Запитом та Технічними вимогами до нього.

   Покупець не розглядає жодних цінових пропозицій, які надходять після кінцевого терміну подання конкурсних пропозицій, встановленого в п. 5 даного Запиту. Пропозиції, отриманні Покупцем після кінцевого терміну подання цінових пропозицій, будуть оголошені такими, що надійшли із запізненням, та відхилені.

4. Цінова пропозиція українською мовою за формою, наведеною у Додатку 3 «Цінова пропозиція» в сканованому вигляді разом з додатковою інформацією мають надсилатися за наступною електронною адресою:

   Міністерство охорони здоров'я України
   Офіс Групи консультаційної підтримки Проекту (ГКПП)
   Ел. пошта: moz.wb.procurement@gmail.com, **обов'язкова копія** на dymytrenko@gmail.com та vorotyuk@outlook.com. В полі «Тема» ел. повідомлення **обов'язково зазначити «HEAL-RFQ-4.1.1.9».**
   Також за зверненням за вищевказаною адресою зацікавленими учасниками може бути отримана довідкова інформація.

5. Кінцевим терміном для отримання пропозицій Покупцем за адресою вказаною в п. 4 вище встановлюється: **31 січня 2024 року, 17:00 за місцевим часом**.

6. До своїх пропозицій Ви маєте додати відповідну документацію, що вимагається Технічними вимогами, вимогами п. 7 (ii) цього Запиту та відповідні відомості, що підтверджують кваліфікацію та досвід надання подібних послуг за формою, наведеною у Додатку 4 «Інформація про досвід та інституційну спроможність» та свідчать про відповідність вимогам визначеним в п. 7 «Кваліфікаційні вимоги» Додатку 2 «Технічні вимоги».

7. Процедура закупівлі – Запит до подання цінових пропозицій відповідно до вимог Правил закупівель Світового банку для позичальників в рамках фінансування інвестиційних проектів (ФІП), в редакції від листопада 2020 року.

   Будь ласка, надайте Ваші цінові пропозиції відповідно до інструкцій у Запиті та Договору, що додається. «Умови постачання» та «Технічні вимоги», що додаються, є складовою частиною Договору.

   **(i) ЦІНИ**. Ціни мають бути виражені в будь-якій валюті, включати ціну товарів на умовах постачання, вказаних у Додатку 1 «Умови постачання», та включати усі обов'язкові платежі (податки, мито, тощо), та вартість додаткових та інших послуг, як зазначено у вищезгаданому Додатку.

   Ціни, що вказані за кожний лот (договір), повинні відповідати 100 % товарних позицій, включених в кожний лот (договір). Ціни, що вказані за кожну товарну позицію лоту, повинні відповідати 100 % від кількості, визначеної для такої позиції лоту.

   **(ii) ДОКУМЕНТАЛЬНЕ ПІДТВЕРДЖЕННЯ АВТОРИЗАЦІЇ ТА ЗАПОБІГАННЯ ФАЛЬСИФІКАТУ.**
   У випадку, якщо учасник не є виробником пропонованих товарів, то з метою запобігання закупівлі фальсифікатів та дотримання гарантій на своєчасне постачання товару у кількості, якості та забезпечення гарантійного терміну, учасник в складі пропозиції надає:

   - копію документу від виробника чи офіційного представника виробника на території України, що засвідчує можливість Учасника поставити товари, які є предметом закупівлі та пропонується таким Учасником, належної якості, у кількості, з підтвердженням відповідної сервісної та гарантійної підтримки впродовж визначеного строку, згідно вимог Запиту до подання цінових пропозицій. Такий документ (автроризаційний лист, договір, чи інше) обов'язково повинен включати номер оголошення (ідентифікатор закупівлі), перелік товарів із зазначенням кількості, а також назву предмету закупівлі та назву Покупця згідно Запиту. Покупець може перевірити статус організації, яка видала авторизаційні документи (*вимога до всіх товарних позицій*).

**(iii) ОЦІНКА ПРОПОЗИЦІЙ.** Пропозиції, які визнані такими, що задовольняють Технічним вимогам та Запиту, оцінюватимуться шляхом порівняння загальної ціни відповідно до встановлених вимог, як вказано в п. (i) вище. У випадку подання цінових пропозицій у іншій валюті, з метою порівняння, Покупець конвертує всі ціни у валюту країни Покупця (українська гривня) по обмінному курсу продажу, опублікованому Національним банком України (https://bank.gov.ua/ua/markets/exchangerates) на дату кінцевого терміну отримання пропозицій, встановленого в п. 5 даного Запиту.

Цінові пропозиції оцінюватимуться за всіма позиціями та договір буде присуджено фірмі, яка запропонувала найменшу оцінену вартість всіх позицій та відповідає усім умовам, встановленим цим Запитом та Технічними вимогами до нього.

При оцінці пропозицій, Покупець визначить для кожної цінової пропозиції оціночну вартість шляхом:

- коригування цінової пропозиції з метою виправлення арифметичних помилок таким чином:

а) якщо у будь-якому місці є невідповідність між сумою цифрами та прописом, сума прописом буде вважатися вірною;

б) якщо у будь-якому місці є невідповідність між ціною за одиницю та загальною сумою, яка обчислюється шляхом перемноження ціни за одиницю на кількість, ціна за одиницю буде вважатися вірною;

в) якщо Постачальник відмовиться прийняти вказані корегування, його цінова пропозиція буде відхилена.

**(iv) ВИЗНАЧЕННЯ ПЕРЕМОЖЦЯ.** Переможцем буде визначено фірму чи учасника фізичну особу-підприємця, яка(ий) запропонує найнижчу загальну ціну та пропозиція якого відповідає умовам, встановленим Технічними та іншими вимогами цього Запиту, зокрема передбаченими п. 7 (ii), (iii) цього Запиту, а Постачальник відповідає встановленим обов'язковим кваліфікаційним вимогам.

**Період очікувань**

Договір може бути присуджено не раніше закінчення Періоду очікувань, який триває 10 робочих днів після дати направлення Покупцем всім учасникам, що подали цінові пропозиції, Повідомлення про намір акцептувати цінову пропозицію переможця. У випадку отримання однієї цінової пропозиції Період очікувань не застосовується.

**Повідомлення про намір акцептувати цінову пропозицію**

У випадку застосування Періоду очікувань він повинен розпочинатись, коли Покупець направив кожному із учасників Повідомлення про намір акцептувати цінову пропозицію переможця. Повідомлення про намір акцептувати цінову пропозицію буде включати щонайменше наступну інформацію:

(a) назву та адресу учасника, що подав цінову пропозицію яка буде акцептована;

(b) загальну вартість цінової пропозиції, що буде акцептована;

(c) назви всіх учасників, що подали свої цінові пропозиції та ціни їх пропозицій у валюті пропозиції та валюті оцінки;

(d) повідомлення про підстави відхилення пропозиції (надається учасникам цінові пропозиції яких відхилено);

(e) дата завершення Періоду очікувань;

(f) інструкцію щодо звернення за роз'ясненнями та/чи подання скарги впродовж періоду очікувань.

**Право Покупця змінювати кількість товарів під час акцепту пропозиції**

Під час акцепту цінової пропозиції Покупець має право на збільшення чи зменшення кількості товару чи супутніх послуг визначених в Додатку 1 «Умови надання послуг» та Додатку 2 «Технічні вимоги» на відсоток, як вказано в Додатку 1, без зміни цін за одиницю, а також інших термінів та умов.

**Повідомлення про акцепт**

До завершення терміну чинності цінових пропозицій але не раніше завершення Періоду очікувань чи іншого продовження цього періоду чи в наслідок задоволення скарги що подана впродовж Періоду очікувань, Покупець направляє повідомлення про акцепт переможцю. В повідомленні про акцепт зазначається сума яку Покупець акцептує та яка буде виплачена постачальнику в наслідок виконання договору (в подальшому ця сума складає вартість договору).

**(v) УКЛАДЕННЯ ДОГОВОРУ.** З обраним Постачальником буде укладено договір за формою, наведеною у Додатку 5 «Договір».

**(vi) ТЕРМІН ЧИННОСТІ ПРОПОЗИЦІЙ:** запропоновані цінові пропозиції повинні бути чинними протягом 60 (шістдесят) календарних днів від дати кінцевого терміну отримання пропозицій, встановленої в п. 5 даного Запиту.

8. **ПЕРЕВІРКИ ТА АУДИТ**

Постачальником повинен виконувати всі вказівки Покупця, які відповідають застосованому законодавству країни Покупця.

Постачальник повинен дозволяти, та забезпечити дозвіл всіх своїх підрядників та консультантів, на перевірку Банком та/або особами призначеними Банком всіх офісів Постачальника та всіх рахунків та документів, пов'язаних з впровадженням Договору та підготовкою цінової пропозиції, та дозволяти перевірку цих рахунків та документів аудитором, призначеним Банком, якщо це вимагатиме Банк. Увага Постачальника та його підрядників та консультантів звертається на статтю 5 «Шахрайство та корупція» Форми Договору, яка передбачає, серед іншого, що дії спрямовані на суттєве перешкоджання реалізації Банком його прав щодо перевірок та аудиту, становлять заборонену практику, яка може бути підставою для розірвання Договору (а також визнання Постачальника неправомочним відповідно до процедур Світового Банку щодо застосування санкцій).

9. Будь ласка, надайте письмове підтвердження (електронною поштою) отримання цього Запиту та Вашої участі у торгах.

**Додатки:**

Додаток 1. Умови надання послуг
Додаток 2. Технічні вимоги
Додаток 3. Цінова пропозиція
Додаток 4. Форма « Інформація про досвід та інституційну спроможність »
Додаток 5. Договір

**ДОДАТОК 1**

до Запиту до подання цінових пропозицій № HEAL-RFQ-4.1.1.9

## УМОВИ НАДАННЯ ПОСЛУГ

Назва пакету: «Забезпечення функціонування Галузевого центру кібербезпеки сфери охорони здоров'я»
Номер пакету: HEAL-RFQ-4.1.1.9
Покупець: Міністерство охорони здоров'я України

### 1. Ціна пропозиції

| № | Найменування послуг (детальний опис наведено в відповідному пункті Технічних вимог) | Одиниця виміру | Кількість | Ціна за одиницю [вказати валюту], без ПДВ | Загальна вартість [вказати валюту], без ПДВ |
|---|---|---|---|---|---|
| 1. | Програмна продукція - Підсистема управління подіями інформаційної безпеки (SIEM+SOAR) на 5000 EPS [вказати склад підсистеми, кількість ліцезій та їх тип] | комплект | 1 | | |
| 2. | Програмна продукція - Підсистема аудиту дій користувачів та надання доступу до критично важливих систем [вказати склад підсистеми, кількість ліцезій та їх тип] | комплект | 1 | | |
| 3. | Програмна продукція - Підсистема для фільтрації мережевого трафіку та захисту мережі, аналізу запобігання мережевих вторгнень [вказати склад підсистеми, кількість ліцезій та їх тип] | комплект | 2 | | |
| 4. | Програмна продукція - Підсистема для забезпечення захисту веб-додатків [вказати склад підсистеми, кількість ліцезій та їх тип] | комплект | 1 | | |
| 5. | Послуги[1] зі встановлення, налаштування та інтеграції програмної продукції вказаної в п. 1-4 | послуга | 1 | | |
| 6. | Навчання персоналу Покупця | послуга | 1 | | |
| | **ЗАГАЛЬНА ВАРТІСТЬ ПРОПОЗИЦІЇ БЕЗ ПДВ** | | | | |
| | **ПДВ** | | | | |
| | **ЗАГАЛЬНА ВАРТІСТЬ ПРОПОЗИЦІЇ З ПДВ** | | | | |

[1] Послуги включають також розробку архітектурних рішень та технічної документації

**Примітка 1:** у разі розбіжності між сумою, підрахованою шляхом перемноження ціни за одиницю на кількість, та загальною ціною, підрахованою учасником торгів, чинною вважається загальна ціна, вирахувана на основі цін за одиницю.

**2. Термін чинності цінової пропозиції**
Запропонована цінова пропозиція є чинною протягом шістидесяти (60) днів від дати кінцевого терміну отримання пропозицій, встановленої в п. 5 Запиту до подання цінових пропозицій.

**3. Фіксована ціна**
Наведені вище ціни за одиницю є фіксованими і жодним змінам не підлягають, включаючи період виконання Договору.

**4. Право Покупця змінювати кількість товарів під час присудження Договору**
Покупець залишає за собою право під час присудження Договору збільшувати або зменшувати на 1-15% кількість товарів, визначених у «Запиті до подання цінових пропозицій» за умови, що не вноситься будь-яких змін до одиничних цін та інших умов надання послуг.

**5. Терміни та умови виконання**
Надання ліцензій та надання Послуг повинно бути здійснено впродовж 5 (пяти) місяців від дати підписання Договору.

**6. Оплата**

Оплата проводиться на умовах вказаних в п. 3 Договору.

**7. Наслідки невиконання договору Постачальником**
Покупець має право розірвати Договір без будь-яких зобов‘язань перед Постачальником якщо Постачальник не усуває недоліки у виконанні своїх зобов'язань за Договором протягом 5 (п’яти) робочих днів після отримання відповідного письмового повідомлення від Покупця

**8. Дефекти та недоліки**
Усі дефекти та недоліки має бути виправлено Постачальником без будь-яких витрат з боку Покупцем протягом 30 днів з дати повідомлення Покупцем про них.

**9. Технічні вимоги**
Детальні технічні вимоги та необхідна кількість/обсяг зазначених вище послуг наведені у Додатку 2 до Запиту. Постачальник має підтвердити відповідність запропонованих послуг специфікаціям по кожній позиції або навести усі розбіжності.

**[НАЗВА ПОСТАЧАЛЬНИКА]**
**Підпис уповноваженої особи:**
**Печатка компанії**
**Місце:**
**Дата:**

**[Примітка:** Будь ласка ПІДПИШІТЬ та поставте ПЕЧАТКУ на ВСІ сторінки цього документу.]

**ДОДАТОК 2**

до Запит до подання цінових
пропозицій № HEAL-RFQ-4.1.1.9

## ТЕХНІЧНІ ВИМОГИ

Назва пакету: «Забезпечення функціонування Галузевого центру кібербезпеки сфери охорони здоров'я»
Номер пакету: HEAL-RFQ-4.1.1.9
Покупець: Міністерство охорони здоров'я України

### 1. ТЕРМІНИ, ВИЗНАЧЕННЯ ТА СКОРОЧЕННЯ

| | |
|---|---|
| ГЦК | Галузевий центр кіберзахисту сфери охорони здоров'я |
| SIEM | Security Information and Event Management. SIEM є рішенням в галузі кібербезпеки, яке об'єднує в собі системи для збору, аналізу та реагування на інформацію про події та безпеку в реальному часі. |
| SOAR | Security Orchestration, Automation, and Response. SOAR використовується в кібербезпеці для автоматизації процесів виявлення та реагування на загрози за допомогою оркестрації і автоматизації. |
| WAF | Web Application Firewall. WAF - це спеціальна система безпеки, яка застосовується для захисту веб-додатків від різноманітних атак та уразливостей. |
| EPS | Events Per Second. EPS вимірює кількість подій, які система або програма може обробляти за секунду. Це важливий параметр для обладнання та програм, які обробляють великі потоки подій, наприклад, у системах безпеки. |
| CLI | Command Line Interface. CLI - це текстовий інтерфейс користувача для взаємодії з комп'ютерною системою шляхом введення текстових команд. |
| SNMP | Simple Network Management Protocol. SNMP - це протокол управління мережами, який дозволяє збирати інформацію про мережеві пристрої та керувати ними в мережі. |
| HTTPS | Hypertext Transfer Protocol Secure. HTTPS - це захищений протокол передачі гіпертекстового контенту через інтернет. Використовує TLS або SSL для шифрування даних між клієнтом та сервером. |
| GUI | Graphical User Interface. GUI - це інтерфейс користувача, який використовує графічні елементи, такі як вікна, кнопки та меню, для взаємодії з користувачем. |
| LDAP | Lightweight Directory Access Protocol. LDAP - це протокол доступу до каталогів, який використовується для управління та запитів інформації з директорій, таких як адресні книги та корпоративні каталоги. |
| XML | eXtensible Markup Language. XML - це мова розмітки, яка використовується для зберігання та обміну даними у структурованому форматі. |

| | |
|---|---|
| WMI | Windows Management Instrumentation. WMI - це інтерфейс для управління компонентами та параметрами операційної системи Windows. |
| API | Application Programming Interface. API - це набір правил та визначень, які дозволяють одному програмному засобу взаємодіяти з іншим програмним засобом. |
| REST | Representational State Transfer. REST - це архітектурний стиль для створення веб-служб, який використовує HTTP протокол для звернення до ресурсів (наприклад, URL), а також CRUD операції (створення, читання, оновлення, видалення) для роботи з цими ресурсами. |
| AD | Active Directory. AD - це служба каталогів, яка використовується у середовищі Windows для управління користувачами, групами та іншими об'єктами мережі. |
| RDP | Remote Desktop Protocol. RDP - це протокол для забезпечення віддаленого доступу до комп'ютерів та інших пристроїв у мережі. |
| SAML | Security Assertion Markup Language. SAML - це мова розмітки для передачі даних про аутентифікацію та авторизацію між сторонами, зокрема між службами одного домену та іншого домену чи службою одного постачальника та іншого постачальника. |

## 2. Загальні відомості

### 2.1 Загальні положення

Стрімкий розвиток інформаційних технологій надає переваги сучасного цифрового світу та розвиток інформаційних технологій, що в свою чергу обумовлює виникнення нових загроз національній та міжнародній безпеці.

Поряд із інцидентами природного (ненавмисного) походження зростає кількість та потужність кібератак, вмотивованих інтересами окремих держав, груп та осіб.

Внаслідок сильної зв'язності інформаційного суспільства, яке не має меж та кордонів, стан захисту об'єктів критичної інформаційної інфраструктури України прямо та опосередковано впливає на інші країни і все більше впливає на імідж України в світовому інформаційному просторі.

Кібератаки на комунікаційну або технологічну систему підприємств, які відносяться до об’єктів критичної інформаційної інфраструктури в галузі охорони здоров’я, безпосередньо впливають на стале функціонування таких об’єктів.

Поширюються випадки незаконного збирання, зберігання, використання, знищення та поширення персональних даних, незаконних фінансових операцій, крадіжок та шахрайства у мережі Інтернет, кібератаки на ключові підприємства критичної інформаційної інфраструктури охорони здоров’я. Кіберзлочинність стає транснаціональною та здатна завдати значної шкоди інтересам особи, суспільства і держави.

Для запобігання розвитку таких подій, підприємства повинні забезпечити проведення аудиту інформаційної безпеки (у тому числі у разі необхідності і на підпорядкованих об'єктах та об’єктах, що належать до сфери їх управління), і як результат - розробити і реалізовувати

запобіжні, організаційні та інші заходи у сфері кібербезпеки, в тому числі шляхом впровадження відповідних технологічних рішень та програмно-апаратних комплексів.

Сучасний стан захищеності інформаційних систем об'єктів критичної інформаційної інфраструктури охорони здоров’я на сьогодні знаходиться на низькому рівні.

Необхідно вжити нижчезазначених заходів в короткі строки з метою упередження можливих майбутніх більш потужних атак. Потрібно готуватися виходячи із міркувань, що зловмисники вже отримали уявлення про внутрішню структуру інформаційних мереж підприємств та установ.

### 2.2 Призначення

З огляду на зазначене потрібно вжити комплекс заходів для мінімізації негативних чинників з метою забезпечення належного рівня інформаційної безпеки галузі охорони здоров’я та суспільства в цілому. Їх можливо поділити на три складові: організаційні, нормативно-правові та технічні.

З метою реалізації цих заходів необхідно створити галузевий центр кібербезпеки в галузі охорони здоров’я.

У цьому документі наведені технічні вимоги до комплектів програмної продукції та супутніх послуг для забезпечення функціонування Галузевого центру кібербезпеки сфери охорони здоров’я.

## 3. Вимоги чинного законодавства

Програмне забезпечення та послуги з його впровадження повинні відповідати вимогам чинних нормативно-правових документів, а саме:

- Закону України «Про інформацію»;
- Закону України «Про захист інформації в інформаційно-комунікаційних системах»;
- Закону України «Про електронні довірчі послуги»;
- Закону України «Про доступ до публічної інформації»;
- постанові Кабінету Міністрів України від 29.03.2006 № 373 «Про затвердження Правил забезпечення захисту інформації в інформаційних, телекомунікаційних та інформаційно-телекомунікаційних системах»;
- постанові Кабінету Міністрів України від 04.02.1998 № 121 «Про затвердження переліку обов’язкових етапів робіт під час проектування, впровадження та експлуатації засобів інформатизації»;
- ДСТУ ISO/IEC/IEEE 12207:2018. Інженерія систем і програмних засобів. Процеси життєвого циклу програмних засобів;
- ДСТУ ISO/IEC/IEEE 15288:2016 Інженерія систем і програмного забезпечення. Процеси життєвого циклу систем (ISO/IEC/IEEE 15288:2015, IDT);
- ДСТУ ISO/IEC 2382:2017 (ISO/IEC 2382:2015, IDT). Інформаційні технології. Словник термінів;
- ДСТУ ISO/IEC 14764:2014. Інженерія програмного забезпечення. Процеси життєвого циклу програмного забезпечення. Технічне обслуговування;

- ДСТУ 4163:2020. Державна уніфікована система документації. Уніфікована система організаційно-розпорядчої документації. Вимоги до оформлення документів;
- ДСТУ 3008:2015 Інформація та документація. Звіти у сфері науки і техніки. Структура та правила оформлювання;
- НД ТЗІ 1.1-003-99. Термінологія в галузі захисту 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;
- ДСТУ 2226-93 Автоматизовані системи. Терміни та визначення.
- Закон України «Про основні засади забезпечення кібербезпеки України» № 2163-VIII від 05.10.2017 р., в редакції від 24.10.2020 р.
- Закон України «Про захист інформації в інформаційно-телекомунікаційних системах» № 80/94-ВР від 05.07.1994 р., в редакції від 04.07.2020 р.
- Закон України «Про електронні документи та електронний документообіг» № 851-IV від 22.05.2003 р., в редакції від 07.11.2018 р.
- Закон України «Про захист персональних даних» № 2297-VI від 01.06.2010 р., в редакції від 23.04.2021 р.
- Постанова Кабінету Міністрів України «Про затвердження переліку об'єктів державної власності, що мають стратегічне значення для економіки і безпеки держави» № 83 від 04.03.2015 р., в редакції від 29.04.2021 р.
- Постанова Кабінету Міністрів України «Про затвердження Загальних вимог до кіберзахисту об'єктів критичної інфраструктури» № 518 від 19.06.2019 р., в редакції від 19.06.2019 р.
- Постанова Кабінету Міністрів України «Деякі питання об'єктів критичної інформаційної інфраструктури» № 943 від 09.10.2020 р., в редакції від 09.10.2020 р.
- Постанова Кабінету Міністрів України «Деякі питання об'єктів критичної інформаційної інфраструктури» № 1109 від 09.10.2020 р., в редакції від 09.10.2020 р.
- ДСТУ ISO/IEC 27000:2019 «Інформаційні технології. Методи захисту. Системи керування інформаційною безпекою. Огляд і словник термінів (ISO/IEC 27000:2018, IDT)» .
- ДСТУ ISO/IEC 27001:2015 «Інформаційні технології. Методи захисту. Системи управління інформаційною безпекою. Вимоги (ISO/IEC 27001:2013/Cor 2:2015, IDT). Поправка № 2:2019».
- ДСТУ ISO/IEC 27002:2015 «Інформаційні технології. Методи захисту. Звід практик щодо заходів інформаційної безпеки (ISO/IEC 27002:2013/Cor 2:2015, IDT). Поправка № 2:2019».
- ДСТУ ISO/IEC 27005:2019 «Інформаційні технології. Методи захисту. Управління ризиками інформаційної безпеки (ISO/IEC 27005:2018, IDT)».
- Серія міжнародних стандартів ISO/IEC 27000 Міжнародної організації зі стандартизації (ISO) та Міжнародної електротехнічної Комісії (IEC), яка включає стандарти інформаційної безпеки та кібербезпеки.

## 4. ВИМОГИ ДО СКЛАДУ ТА ФУНКЦІОНАЛЬНОСТІ

### 4.1. Система кібез захисту включає в себе наступні підситеми

I - Програмна продукція - Підсистема управління подіями інформаційної безпеки (SIEM+SOAR) на 5000 EPS: – 1 комплект

II. Програмна продукція - Підсистема аудиту дій користувачів та надання доступу до критично важливих систем– 1 комплект.

III. Програмна продукція - Підсистема для фільтрації мережевого трафіку та захисту мережі, аналізу запобігання мережевих вторгнень– 2 комплекти.

IV. Програмна продукція - Підсистема для забезпечення захисту веб-додатків – 1 комплект

### 4.2. Програмна продукція - Підсистема управління подіями інформаційної безпеки (SIEM+SOAR) на 5000 EPS: – 1 комплект

#### 4.2.1. Загальні вимоги Покупця до програмної продукції

Підсистема призначена для управління інформаційною безпекою та подіями безпеки. Забезпечує аналіз в реальному часі подій (тривог) безпеки, отриманих від мережевих пристроїв і додатків та кореляцію цих подій. Також використовується для журналювання даних і генерації звітів в цілях сумісності з іншими бізнес-даними. Підсистема проводить реєстрацію даних безпеки та створення звітів для цілей відповідності. Якщо відповідно до функціональності системи або згідно архітектурного підходу реалізація технічних вимог потребує додаткових модулів або ліцензій, то все це має бути закладено в комплект поставки з урахуванням вимог до строку та функціональності технічної підтримки.

Всі необхідні ліцензії для забезпечення зазначеного в цих вимогах функціоналу та кількісних показників продуктивності мають бути у комплекті запропонованого рішення.

Підсистема має бути реалізована на основі масштабованої, розподіленої архітектури (розподілене розгортання елементів) та включати в себе:

- ядро системи, що здійснює основний функціонал SIEM (обробку, аналітику, тощо);
- елементи автоматизації реакції на інциденти (SOAR);
- елемент збору та обробки подій з журналів подій;
- елементи збору подій, що пересилають події у ядро або модуль обробки журналів подій**.**

#### 4.2.2. Архітектура підсистеми

4.2.2.1. Підсистема має бути у вигляді віртуалізованого рішення (VMWare/Hyper-V/KVM) та розміщена на сайті/потужностях Покупця.

4.2.2.2. Підсистема повинна мати можливість приймати події при навантаженні не менш ніж 5000 подій на секунду (Events Per Second), при короткочасному збільшенню подій більше заданого значення події не повинні втрачатися та обробляються поза піковим навантаженням.

4.2.2.3. Підсистема повинна мати можливість масштабування кількості обробки подій на секунду з урахування збільшення або зменшення кількості джерел подій без необхідності придбання додактових ліцензій зі сторони Покупця.

4.2.2.4. Підсистема повинна забезпечувати зберігання подій у «сирому» вигляді для використання в якості доказової бази

4.2.2.5. Підтримка масштабування сховища даних для зберігання оперативних та архівованих подій

4.2.2.6. Підтримка автоматизованого процесу архівації події, що не вимагає втручання адміністратора та налаштовується через графічний інтерфейс

4.2.2.7. Підтримка можливості масштабування шляхом додавання нових віртуальних машин в кластер вже розгорнутих елементів та проводитись без перевстановлення рішення

4.2.2.8. Можливість управління додатковими модулями рішення проводиться через єдиний графічний веб-інтерфейс

4.2.2.9. Можливість автоматизованого резервного копіювання конфігурації рішення

4.2.2.10. Можливість розподілення навантаження (load balancing) та відмовостійкості (redundancy)

4.2.2.11. Підтримка використання компресії подій з метою зменшення кількості однотипних подій

4.2.2.12. Можливість проведення внутрішнього управління інцидентами з оповіщенням по електронній пошті, веб-інтерфейсу, призначенням відповідальних осіб і відстеженням життєвого циклу інциденту

4.2.2.13. Рішення повинно підтримувати шифрування інформації, переданої між рознесеними модулями/вузлами

4.2.2.14. Наявність у складі рішення усіх необхідних ліцензій для бази даних з урахуванням можливого росту подій у відповідності до цих вимог.

### 4.2.3. Ліцензування

Підсистема має бути ліцензована для прийому подій сумарно не менше ніж 5000 EPS, які будуть піддаватися кореляції в режимі «реального часу».

У разі ліцензування для прийому подій система повинна ліцензуватися по середньому показнику EPS за добу протягом 45 днів та не мати обмежень на кількість максимально оброблених або пікових EPS

Усі ліцензії повинні бути безстроковими та не мати дати закінчення (perpetual).

### 4.2.4. Вимоги до підсистеми

Підтримка можливості збільшення потужності елементів системи (ядра, збору подій, аналітики та кібер-криміналістики);

Підтримка можливісті стиснення даних перед пересиланням на рівень зберігання і на рівень ядра.

Підсистема має забезпечувати веб-інтерфейс, клієнтське ПЗ та командну строку CLI для адміністративного доступу

### 4.2.5. Функціональність підсистеми

4.2.5.1. налаштування правил кореляції в режимі «реального часу»;
4.2.5.2. налаштування графічних панелей візуалізації (Dashboards);
4.2.5.3. створення системних звітів;
4.2.5.4. створення та контроль панелей візуалізації і звітів щодо відповідності стандартам (compliance). Створення повинно відбуватись за допомогою додаткових пакетів готових правил кореляції відповідності стандартам (Compliance Insight Packages - CIP). Повинні бути пакети правил кореліції для наступних стандартів: PCI-DSS та HIPAA.

4.2.5.5. впровадження правил кореляції згідно матриці MITRE (https://attack.mitre.org/) шляхом технологічного імпорту готових пакетів правил кореляції, дашбордів, тощо, створених виробником;

4.2.5.6. створення правил автоматизації реакції на кібер-загрози (playbook) у графічному інтерфейсі модуля SOAR;

4.2.5.7. Підсистема повинна підтримувати вбудовані механізми створення і обробки карток інцидентів.

### 4.2.6. Збір подій

Модулі збору повинні бути реалізовані як системні служби ОС, що функціонують спільно з іншими компонентами Підсистеми на сервері (-ів) Підсистеми збору, зберігання і аналізу подій ІБ або функціонують на виділеному сервері (-ів) модулів збору і / або на серверах цільових систем.

Модулі збору повинні забезпечувати виконання таких основних функцій:

4.2.6.1. збір подій безпеки з журналів реєстрації цільових систем;
4.2.6.2. нормалізація подій;
4.2.6.3. категоризація подій;
4.2.6.4. збагачення подій додатковою інформацією;
4.2.6.5. фільтрація і агрегація подій;
4.2.6.6. пріоритизація подій;
4.2.6.7. тимчасове зберігання (кешування) подій в разі недоступності одержувача даних;
4.2.6.8. передача подій.

Збір подій безпеки з журналів реєстрації цільових систем повинен здійснюватися в наступних режимах:

- в режимі автоматичного опитування (періодичне читання подій з файлу, періодична вибірка подій з таблиць бази даних і т.п.)
- в режимі отримання повідомлень (отримання повідомлень про події ІБ по протоколу syslog, SNMP і т.п.).

Збір подій повинен виконуватися віддалено (без установки агентів на кінцеві системи) з використанням підтримуваних джерелами протоколів передач.

Збір подій повинен виконуватися в режимі близькому до режиму реального часу. Події безпеки повинні збиратися в Підсистему в міру їх реєстрації, з мінімальною затримкою часу між реєстрацією події в вихідному журналі і його надходженням в Систему.

### 4.2.7. Нормалізація подій

4.2.7.1. Модулі збору повинні здійснювати нормалізацію зібраних подій безпеки. При нормалізації зібраних подій безпеки повинен виконуватися розбір вихідних подій безпеки на поля і запис отриманих полів в поля уніфікованого формату. При нормалізації зібраних подій безпеки в одному з полів нормалізованого вигляду при необхідності має зберігатися вихідна подія, яка була нормалізована.

4.2.7.2. Модулі збору повинні надавати можливість створення власних правил нормалізації, а також функціонал по перевизначення логіки роботи вбудованих правил

4.2.7.3. Підсистема повинна надавати графічні інструменти для створення власних правил нормалізації

4.2.7.4. Зберігання подій в Підсистемі має здійснюватися в нормалізованому вигляді з можливість збереження подій у вихідному форматі

### 4.2.8. Кешування

4.2.8.1. Модулі збору повинні забезпечувати можливість тимчасового зберігання зібраних подій безпеки (буферизацію)

4.2.8.2. При втраті зв'язку з іншими модулями Підсистеми всі зібрані події повинні поміщатися в буфер модулів збору

4.2.8.3. Модулі збору повинні надавати можливість налаштування розміру буфера для зберігання зібраних подій безпеки

4.2.8.4. Модулі збору повинні використовувати незалежні буфери для кожного модуля призначення

### 4.2.9. Зберігання та звітність

Модуль зберігання і звітності повинен забезпечувати виконання таких основних функцій:

- отримання подій
- зберігання подій
- функції пошуку і візуалізації
- звітність по збереженим подіям
- передача подій в інші модулі системи

При отриманні подій безпосередньо від джерел повинні підтримуватися наступні формати і протоколи:

- CEF syslog (UDP, TCP)
- Syslog (UDP, TCP)
- Текстові файли з мережевих сховищ (NFS, CIFS, SAN)
- Текстові файли з віддалених серверів (SCP, SFTP, FTP)

4.2.9.1. При читанні інформації з текстових файлів повинні підтримуватися події аудиту як в однорядковому, так і в багаторядковому форматі.

4.2.9.2. Модуль повинен мати механізм захисту цілісністі збережених журналів подій та надавати в інтерфейсі функціонал перевірки цілісності.

4.2.9.3. Модуль зберігання повинен підтримувати поділ подій на логічні групи (за різними джерелами подій) і настройку для них різних політик по часу зберігання.

4.2.9.4. Налаштування політики зберігання повинно дозволяти керувати як терміном зберігання подій в режимі онлайн, так і зберігання архівних подій.

4.2.9.5. Модуль повинен використовувати індексацію полів і повнотекстову (full-text) індексацію для збільшення продуктивності пошуку. Адміністратору системи повинна надаватися можливість настройки індексованих полів.

4.2.9.6. Модуль зберігання повинен підтримувати функціонал, що забезпечує налаштування підвищеного рівеня індексації для обмеженого набору полів.

4.2.9.7. Підсистема повинна забезпечувати високу ступінь стиснення збережених подій (не менше п'ятикратного) без втрати функціоналу пошуку по ним і історичної кореляції.

4.2.9.8. Модуль зберігання повинен підтримувати розподілене зберігання подій на декількох зразках і зберігати можливість пошуку за всіма даними з єдиного інтерфейсу.

4.2.9.9. Модуль повинен надавати можливість пошуку по збереженим подій і їх візуалізації.

4.2.9.10. Модуль повинен підтримувати складання пошукових запитів по нормалізованим полях, а також використовуючи повнотекстовий (full text) пошук.

4.2.9.11. Має підтримуватися складання пошукових запитів з використанням спеціальної мови і з використанням графічного конструктора.

4.2.9.12. Функціонал пошуку повинен підтримувати використання вбудованих операторів для реалізації наступного набору аналітичних можливостей:

- графічне представлення даних
- наявність базових аналітичних функцій (count, sum, avg, min, max, stdev, percent)
- функції агрегації і угруповання по довільним критеріям
- виключення повторюваних значень
- вказівка винятків до критеріїв пошуку (по полях)
- обмеження результатів виведення (head, tail)
- сортування результатів по довільним критеріям
- можливість використання зовнішніх списків в якості критеріїв пошуку і для збагачення виведених результатів
- можливість використання регулярних виразів (regex) в якості критеріїв пошуку
- функції витягів (нормалізації) полів, при роботі з raw-подіями

4.2.9.13. При використанні архітектури розподіленого зберігання модуль повинен надавати можливість як локального, так і розподіленого пошуку.

### 4.2.10. Відмовостій-кість та резервування

4.2.10.1. резервування ядра системи (засобами віртуалізації/гіпервізора або вбудованим функціоналом в елементи ядра);

4.2.10.2. резервування елементів збору подій (засобами віртуалізації/гіпервізора або вбудованим функціоналом в елементи збору або застосуванням елементів балансування);

4.2.10.3. збереження подій локально на елементах збору, якщо відсутній зв'язок з ядром та системою зберігання даних;

4.2.10.4. резервування та відновлення конфігурації системи;

4.2.10.5. відновлення бази даних системи після збоїв.

### 4.2.11. Захищеність підсистеми

Підсистема повинна відповідати наступним вимогам:

- обмеження доступу до даних і інтерфейсу управління на основі ролей (RBAC)
- автентифікація адміністративного доступу: локальна, LDAP, Radius
- підтримка 2FA (Two-factor authentication)
- безпечні протоколи передачі даних між компонентами системи (HTTPS, TLS)

### 4.2.12. Управління подіями і даними

4.2.12.1. нормалізація подій (перетворення записів журнальних файлів у єдиний стандартний вигляд)

4.2.12.2. модернізація та додавання категорій нормалізації

4.2.12.3. агрегація подій (об'єднання однакових подій)

4.2.12.4. керування правилами кореляції

4.2.12.5. фільтрація подій (запис подій, які відповідають певним умовам)

4.2.12.6. пошук подій на основі ключових слів і атрибутів подій

4.2.12.7. пошук подій в режимі реального часу

4.2.12.8. контроль цілісності подій

4.2.12.9. збір, зберігання та робота з “raw”-подіями

4.2.12.10. зберігати як необроблений масив подій (у початковому вигляді), так і оброблений/нормалізований масив подій

4.2.12.11. зберігання даних протягом різного періоду часу

4.2.12.12. система повинна підтримувати можливості збору додаткової інформації, крім журналів подій пристроїв

4.2.12.13. “без агентський” методи збору подій з джерел

4.2.12.14. підтримка різних форматів збору подій (syslog, CEF, WMI, SQL, txt, тощо)

4.2.12.15. збір даних про мережевий трафік на основі NetFlow/sFlow/j-Flow/IPFIX

**4.2.13. Обробники подій (parsers)**

- автоматичне оновлення обробників подій
- модифікація і кастомізація обробників подій
- створення та модифікації власних обробників подій за допомогою GUI
- опис обробників подій за допомогою XML

**4.2.14. Агентське ПЗ (для Windows)**

Підсистема повинна підтримувати можливості збору подій Windows через WMI і за допомогою агентського ПЗ.

**4.2.15. Візуалізація і аналітика**

Підсистема повинна підтримувати наступні функції:

- фільтрація по полям
- створення та модернізація візуальних панелей користувачів (Custom Dashboards)
- інтерактивна робота з візуальними панелями (Drill-down into dashbords)
- вбудований конструктор звітів
- формування звітів у вигляді документів наступних форматів (PDF, HTML, CVS, тощо)
- формування та відправка звітів по email за розкладом або за правилами
- експорт та імпорт правил (rules) і звітів (reports) за допомогою XML

**4.2.16. Управління інцидентами та вразливостями**

Підсистема повинна підтримувати:

- механізми аналітики та управління інцидентами в реальному часі, що спрацьовують відповідно до комплексних шаблонів подій на основі правил
- ведення картки інциденту

- можливість автоматичного застосування запрограмованих дій в разі виникнення інциденту
- система повинна підтримувати можливість поширення повідомлень (сповіщення) про інциденти на основі політик
- можливості виклику скриптів виправлення при виникненні специфічних інцидентів
- можливості інтеграції на основі API з зовнішніми системами розподілу заявок (Service Desk / Ticketing systems)
- сортування вразливостей за різними критеріями
- можливість виділення помилкових спрацьовувань
- сповіщення про інциденти по email, через консоль, SNMP, XML, тощо

**4.2.17. Інтеграція з зовнішніми джерелами інформації щодо загроз (Threat Intelligence)**

Має включати:

4.2.17.1. API для інтеграції з зовнішніми джерелами інформації щодо загроз.

4.2.17.2. Вбудовану інтеграцію з популярними джерелами інформації щодо загроз. Повинна підтримуватись щонайменьше наступні джерела інформації: ThreatStream, CyberArk, SANS, Zeus, ThreatConnect, Cisco Talos, AlienVault.

4.2.17.3. Підтримку STIX та TAXII

**4.2.18. Інтеграція з зовнішніми системами, розширення даних щодо інцидентів**

Підтримка:

- нативної інтеграції з системою поведінкової аналітики (UEBA), що застосовує механізми автоматичного машинного навчання (Unsupervised Machine Learning)
- інтеграції зі службами каталогів
- прийому даних з іншого рішення типу SIEM
- інтеграції з ITSM / CMDB
- REST API / WEB API
- імпорт індикаторів компроментації (Indicator of compromise , IoC)
- підключення репутаційних баз по IP

**4.2.19. Технічна сервісна підтримка**

Технічна сервісна підтримка не менше ніж 36 місяців з рівнем підтримки 24*7.

Постійний авторизований доступ до сайту виробника 24*7.

Отримання актуальних репутаційних баз, Mitre, сигнатур захисту та сигнатур для сервісів безпеки.

Отримання основних та проміжних релізів програмного забезпечення через сайт підтримки виробника.

**4.2.20. Послуги впровадження**

Постачальник повинен виконати інсталяційні роботи, які повинні включати: підготовчі роботи, інсталяційні роботи, тестування та навчання спеціалістів Покупця, для цього він повинен мати достатню кількість сертифікованих інженерів (з додаванням сертифікатів)

### 4.3. II. Програмна продукція – Підсистема аудиту дій користувачів та надання доступу до критично важливих систем– 1 комплект.

#### 4.3.1. Загальні (системні) вимоги

Підсистема повинна поставлятися в вигляді віртуального пристрою) (VMWare/Hyper-V/KVM) та розміщена на сайті/потужностях Покупця . Тип поставки повинен бути виконаний в вигляді єдиної платформи, що не потребує використання будь-якого стороннього системного або прикладного програмного забезпечення (операційних систем, програмних додатків, систем керування базами даних тощо) для його імплементації.

Підсистема повинна мати вбудований механізм захисту від несанкціонованого доступу інформації що зберігається. Даний захист повинен забезпечувати використання спеціального ключа захисту (пароля або аппаратного ключа) під час кожного запуску Підсистеми (після вимкнення або перезавантаження)

Налаштування та адміністрування Підсистемою повинно виконуватись через окремий веб-портал адміністрування за допомогою будь-якого сучасного браузера (IE, Mozila, Chrome, Opera тощо) без необхідності встановлення додаткових компонентів (плагінів, додатків тощо). Використання веб-консолі на базі технологій Flash або Java (JRE) не допускається

Адміністрування Підсистеми повинно підтримувати рольову модель керування та нагляду за привілейованими користувачами.

Підсистема повинна надавати привілейованим користувачам спеціальний додатковий веб-портал(-и) для доступу к контрольованим (цільовим) системам. Використання даного порталу повинно бути опціональним (не обов’язковим), тобто Підсистема повинна забезпечувати доступ до контрольованих (цільових) системам в тому числі й без такого порталу (за допомогою використання спеціалізованих додатків: Microsoft Remote Desktop Client, Putty client, SQL Developer, Microsoft SQL Management Studio тощо)

Підсистема повинна мати можливість створення відмовостійких конфігурацій на базі вбудованих технологій, використання сторонніх (зовнішніх) засобів для побудови таких (відмово стійких) конфігурацій – не допускається

Підсистема повинна мати вбудовані системи діагностування що пов’язані з помилками доступу до контрольованих (цільових) систем.

- Підсистема повинна мати функціонал збереження та обробки всіх подій, що пов’язані з роботою Підсистеми, а також – функціонал автоматичної передачі таких подій в зовнішні системи обробки подій.
- Підсистема повинна мати вбудований функціонал створення резервних копій що мають включати в себе всі параметри та налаштування, а також записані сесії привілейованих користувачів. Створені такі копії повинні бути захищені від несанкціонованого доступу.
- Підсистема повинна мати функціонал керування різноманітними об’єктами такими як користувачі, цільові системи, способи підключення як локально (за допомогою веб-порталу) так й віддалено (за допомогою відкритих API-інтерфейсів).
- Інтерфейс Підсистеми повинен бути доступний на англійській та українській (або російській) мові.

#### 4.3.2. Ліцензування

Підсистема має бути ліцензована для роботи протягом 36 місяців.

### 4.3.3. Функціональні (технічні) вимоги

4.3.3.1. Підсистема повинна підтримувати запис дій привілейованих користувачів вбудованими засобами без необхідності встановлення будь-якого компоненту (агенту, сервісу, драйверу тощо) як на кінцеві робочі точки привілейованих користувачів, так й на системи до яких підключаються привілейовані користувачі (цільові системи)

4.3.3.2. Підсистема повинна мати вбудований функціонал розпізнавання текстової інформації в записаних графічних сесіях (OCR механізм або аналог), в тому числі – кириличні символи, з метою подальшого пошуку такої інформації.

4.3.3.3. Функціонал (розпізнавання текстової інформації в записаних графічних сесіях) повинен працювати як в ручному режимі так й в автоматичному (застосовуватися до кожної збереженої сесії без втручання адміністратора Підсистеми)

4.3.3.4. Підсистема повинна підтримувати різні схеми імплементації в інфраструктуру Покупця, щонайменше:

• імплементація в вигляді «міст» (в фізичному розриві мережевого трафіку)

• імплементація в вигляді примусової маршрутизації сесій привілейованих користувачів на цільові системи

4.3.3.5. Функціонал Продукту повинен підтримувати розширені мережеві налаштування, такі як:

• підтримка віртуальних мереж (VLAN)

• агрегація мережевих каналів

• створення власних таблиць ARP

• налаштування статичної маршрутизації для окремих мереж

4.3.3.6. Підсистема повинна мати функціонал використання паролів для підключення до цільових систем що зберігаються в сторонніх (зовнішніх) сховищах паролів. Обов’язкова підтримка наступних типів зовнішніх сховищ паролів:

• Lieberman Enterprise Random Password Manager

• CyberArk Enterprise Password Vault

• Hitachi ID Privileged Access Manager

4.3.3.7. Підсистема повинна мати вбудовану панель інформування про статус працездатності та навантаження на компоненти Підсистеми, щонайменше:

• активність дискової системи

• навантаження на процесор(-и)

• навантаження на оперативну пам’ять

• навантаження мережеві компоненти

Така панель інформування повинна бути доступна тільки для адміністраторів Підсистеми на відповідному веб-порталі адміністрування.

4.3.3.8. Підсистема повинна мати можливість роботи з не менш ніж вісьмома віртуальними (в разі використання віртуального пристрою) та не менш чотирма (в разі фізичного пристрою) мережевими адаптерами

4.3.3.9. Кожному мережевому адаптеру Підсистема повинна мати можливість присвоювати унікальну IP-адресу (в тому числі – з різних мережевих сегментів) як в статичному режимі, так й – динамічному (за допомогою DHCP сервісу)

4.3.3.10. Для кожної такої унікальної IP-адреси Підсистема повинна мати можливість присвоювати привілейованим користувачам спеціальний окремий веб-портал для доступу к контрольованим (цільовим) системам

4.3.3.11. Підсистема повинна мати функціонал сегментації доступу до таких веб-порталів на основі груп користувачів та цільових систем

4.3.3.12. Кожен веб-портал для привілейованих користувачів повинен надавати привілейованим користувачам наступні можливості:

• перелік доступних для підключення цільових систем з можливістю відкриття сесій за допомогою стандартних клієнтів (для RDP, VNC та SSH протоколів)

• перелік доступних для підключення цільових систем з можливістю відкриття сесій за допомогою вбудованого WEB клієнта (для SSH, RDP протоколів)

• перелік IP-адрес та портів цільових систем

• тип протоколу що використовується для підключення до цільової системи

• перегляд паролю до цільової системи (в разі якщо такі права надані привілейованому користувачу відповідною парольною політикою)

• зміна пароля на веб-портал для власного облікового запису (в разі якщо пароль зберігається в власному захищеному сховищі Підсистеми)

4.3.3.13. Підсистема повинна мати вбудоване захищене сховище для зберігання записаних сесій привілейованих користувачів, реквізитів доступу (логін, пароль, ключі, доменні імена тощо) до Підсистеми та цільових систем та журналів подій.

4.3.3.14. Захищене сховище повинно використовувати стандартні крипто алгоритми рівня не нижче AES-256.

4.3.3.15. Ролева модель використання Підсистеми повинна забезпечувати наступні розмежування на базі різних облікових записів:

• повні права адміністрування – в тому числі – можливість конфігурування Продукту

• частково обмежені права адміністрування – будь-які дії крім конфігурування Продукту

• обмежені права адміністрування – можливість налаштувань та подальшого нагляду за конкретно заданими цільовими системами та привілейованими користувачами

• права користувача - можливість тільки підключення до заданих цільових систем без можливості входу до веб-порталу адміністрування

4.3.3.16. Підсистема повинна мати функціонал додавання адміністраторів через веб-портал адміністрування Підсистеми з можливістю вибору ролі, строку дії облікового запису, мови та способу автентифікації адміністратора

4.3.3.17. Для кожного облікового запису адміністратора повинна бути підтримка одночасно кількох способів аутентифікації, щонайменше:

• за допомогою статичного паролю що зберігається в захищеному сховищі Підсистеми

• одноразового паролю що генерується зовнішніми сервісами (наприклад, RADIUS-сервером)

• за допомогою зовнішнього каталогу користувачів (AD/LDAP)

• за допомогою SSH ключа

• за допомогою сертифіката чи смарт-карти

• повинен мати функціонал MFA з можливістю альтернативних методів аутентифікації (OTP, SMS, DUO)

• З можливістю використання OATH (з підтримкою різних додатків) для доменних облікових записів

• RADIUS підтримка інтеграції з іншими MFA рішеннями

4.3.3.18. Підсистема повинна мати функціонал додавання привілейованих користувачів через веб-портал адміністрування Підсистеми з можливістю вибору ролі, строку дії облікового запису, мови та способу автентифікації адміністратора.

4.3.3.19. Підсистема повинна мати функціонал додавання привілейованих користувачів такими способами:

• в ручному режимі

• синхронізація з існуючого каталогу користувачів (AD/LDAP)

• через API інтерфейс

4.3.3.20. Для кожного облікового запису привілейованого користувача повинна бути підтримка одночасно кількох способів аутентифікації, щонайменше

• за допомогою статичного паролю що зберігається в захищеному сховищі Продукту

• одноразового паролю що генерується зовнішніми сервісами (наприклад, RADIUS-сервером)

• за допомогою зовнішнього каталогу користувачів (AD/LDAP)

• за допомогою SSH ключа

• за допомогою сертифіката чи смарт-карти

• повинен мати функціонал MFA з можливістю альтернативних методів аутентифікації (OTP, SMS, DUO)

• З можливістю використання OATH (з підтримкою різних додатків) для доменних облікових записів

• RADIUS підтримка інтеграції з іншими MFA рішеннями

4.3.3.21. Підсистема повинна підтримувати не менше трьох одночасних систем зовнішньої автентифікації привілейованих користувачів та адміністраторів Підсистеми, серверів каталогів користувачів AD та LDAP.

4.3.3.22. Для кожного серверу каталогу користувачів (AD або LDAP) Підсистема повинна мати можливість задавати пріоритет використання (по відношенню до інших таких серверів) та наступні параметри:

• ім'я та пароль користувача що має доступ на читання груп користувачів на сервері каталогу користувачів AD та LDAP

• організаційну групу (OU) в каталозі користувачів в якій потрібно шукати привілейованих користувачів

• адресу (FQDN або IP) та порт серверу каталогу користувачів

• можливість використання шифрованого (безпечного) з'єднання за допомогою сертифікатів

4.3.3.23. Підсистема повинна мати функціонал автоматичного надання окремим групам привілейованих користувачів доступу до пулу цільових систем на базі заданої організаційної групи (OU) на сервері каталогу користувачів (AD або LDAP).

4.3.3.24. Підсистема повинна обов'язково мати функціонал створення безпечних (шифрованих) каналів зв'язку на основі сертифікатів SSL між привілейованими користувачами та Підсистемою та між Підсистемою та цільовими системами.

4.3.3.25. Створення таких безпечних (шифрованих) каналів зв'язку повинно створюватися на основі як само підписних сертифікатів (за допомогою пари «відкритий»-«приватний» ключі), так й на основі сертифікатів центру сертифікації (CA).

4.3.3.26. Підсистема повинна надавати можливість перегляду вмісту сертифікатів («відкритої» частини) з можливістю перегляду хеш-сум за алгоритмами MD5 та SHA1.

4.3.3.27. Додавання цільових систем, сесії привілейованих користувачів до яких будуть контролюватися, повинно виконуватися за допомогою відповідного меню в веб-панелі адміністрування, при цьому Підсистема повинна мати функціонал:

• одиночного додавання цільових серверів (за IP-адресою або FQDN, мережевою маскою та портом);

• групового додавання цільових систем (за допомогою мережевої маски накладеної на пул IP-адресів

• Групового додавання цільових систем за допомогою відкритих API-інтерфейсів

4.3.3.28. Підсистема повинна мати функціонал вибору нумерації портів по яким підключаються привілейовані користувачі та портів по яким виконується підключення до цільових систем, тобто, адміністратор Підсистеми повинен мати

можливість примусової зміни портів підключення для привілейованих користувачів для кожної окремої або групи цільових систем.

4.3.3.29. Підсистема повинна підтримувати роботу з цільовими системами, автентифікація привілейованих користувачів на яких виконується наступним чином:

• за допомогою введення локального облікового запису

• за допомогою введення доменного облікового запису

• за допомогою SSH-ключа

4.3.3.30. Підсистема повинна мати наступні можливості роботи з реквізитами доступу (логіни, паролі, ім’я домену, ключі SSH тощо) що використовуються привілейованими користувачами для підключення до цільових систем:

• ручне створення та зберігати реквізитів доступу в захищеному сховищі Підсистеми

• автоматичне додавання, за допомогою сканування облікових записів в AD

• використання зовнішніх систем аутентифікації (в тому числі – зовнішніх спеціалізованих сховищ паролів)

• анонімний доступ (без необхідності введення реквізитів доступу)

4.3.3.31. В разі ручного чи автоматичного створення та зберігання реквізитів доступу для підключення до цільових систем, Підсистема повинна мати функціонал повного маскування від привілейованих користувачів даних реквізитів (крім випадків де такий перегляд дозволено окремою парольною політикою).

4.3.3.32. Підсистема повинна забезпечувати функціонал додаткової (повторної) примусової автентифікації на цільових системах навіть в разі якщо реквізити доступу привілейованих користувачів на Підсистемі та на цільових системах повністю співпадають

4.3.3.33. Підсистема повинна мати можливість примусової зміни паролів на окремих цільових системах за заданою парольною політикою для окремо заданих облікових записів привілейованих користувачів.

4.3.3.34. Така парольна політика повинна забезпечувати наступні можливості:

• довжина пароля

• складність пароля (в тому числі, вимоги до великих літер, цифрових символів, спеціальних символів)

• частота зміни пароля

4.3.3.35. Примусова зміна паролів відповідно до заданої парольної політики повинна підтримуватися щонайменше на таких цільових системах:

• Unix/Linux-based операційні системи (через SSH)

• Windows операційні системи (через WMI)

• Cisco системи (через SSH)

4.3.3.36. Функціонал безпечного обміну паролями між програмними додатками буде перевагою.

4.3.3.37. Підсистема повинна мати вбудований функціонал оцінювання ефективності роботи з цільовими системами як окремих привілейованих користувачів так й груп привілейованих користувачів.

4.3.3.38. Функціонал ефективності роботи з цільовими системами повинен надавати статистику активних дій привілейованих користувачів (час активної роботи по відношенню до загального часу роботи з цільовою системою) можливістю деталізації та експорту статистики в зовнішній звіт

4.3.3.39. Створення резервних копій повинно використовувати шифрований (захищений) протокол обміну даними (наприклад, на базі пари відкритого та приватного SSH ключа).

4.3.3.40. Створені резервні копії повинні бути захищені від несанкціонованого перегляду даних що в них зберігаються та несанкціонованого відновлення.

4.3.3.41. Підсистема повинна мати систему збереження та обробки подій в вигляді журналів що зберігаються в захищеному сховищі.

4.3.3.42. Всі журнали подій повинні бути захищені від модифікації або видалення, в тому числі адміністраторами Підсистеми з найвищими рівнями доступу (правами).

4.3.3.43. Журнали подій повинні включати щонайменше наступну інформацію:

- події пов’язані з працездатність Продукту (в тому числі – журнали налагоджувань)
- події пов’язані з роботою привілейованих користувачів на цільових системах
- події пов’язані з адмініструванням Продукту

4.3.3.44. Підсистема повинна мати можливість експорту повного або часткового журналу подій в зовнішній файл текстового формату. Частковий експорт повинен здійснюватися за різноманітними критеріями, за такими як обліковий запис привілейованого користувача(-ів), тип події, ім’я цільової системи, дата тощо.

4.3.3.45. Підсистема повинна мати інтеграцію з зовнішніми системами обробки подій за допомогою стандартних протоколів, таких як SNMP, syslog тощо.

4.3.3.46. Підсистема повинна мати функціонал цифрового підпису записаних сесій спеціальними ключами/сертифікатами від довірених постачальників таких ключів/сертифікатів з метою гарантування незмінності даних.

4.3.3.47. Підсистема повинна мати можливість інтеграції з системами обліку роботи користувачів (ticketing systems) типу ServiceNow або аналог.

### 4.3.4. Вимоги до функціоналу контролю привілейованих користувачів

4.3.4.1. Підсистема повинна забезпечувати контроль привілейованих користувачів що підключаються до цільових систем по протоколу RDP

4.3.4.2. Підсистема повинна мати можливість контролювати підключення в різних режимах роботи протоколу RDP, в тому числі – в режимах Enhanced RDP Security (TLS) та NLA

4.3.4.3. Підсистема повинна мати функціонал щодо примусового обмеження роздільної здатності та глибини кольору сесії RDP, примусового вимкнення буферу обміну,

обмеження доступу до цільової системи пристроям, обмеження щодо роботи з мультимедійними налаштуваннями

4.3.4.4. Результатом контролю привілейованих користувачів що підключаються до цільових систем по протоколу RDP повинен бути записаний графічний відеоматеріал (відеоролик)

4.3.4.5. Підсистема повинна мати функціонал експорту збережених графічних відеоматеріалів (відеороликів) в зовнішні відео формати AVI, FLV, MPEG з заданою роздільною здатністю

4.3.4.6. Підсистема повинна підтримувати публікацію сторонніх програмних засобів за допомогою функціоналу Remote App по протоколу RDP

4.3.4.7. Підсистема повинна мати можливість контролювати підключення в різних режимах роботи протоколу RDP, в тому числі – в режимах Enhanced RDP Security (TLS) та NLA

4.3.4.8. Підсистема повинна мати функціонал щодо примусового обмеження роздільної здатності та глибини кольору сесії RDP, примусового вимкнення буферу обміну, обмеження доступу до програмного засобу пристроям, обмеження щодо роботи з мультимедійними налаштуваннями

4.3.4.9. Результатом контролю привілейованих користувачів що підключаються до опублікованих програмних засобів по протоколу RDP повинен бути записаний графічний відеоматеріал (відеоролик)

4.3.4.10. Підсистема повинна мати функціонал експорту збережених графічних відеоматеріалів (відеороликів) в зовнішні відео формати AVI, FLV, MPEG з заданою роздільною здатністю

4.3.4.11. Підсистема повинна забезпечувати контроль привілейованих користувачів що підключаються до цільових систем по протоколу SSH

4.3.4.12. Підсистема повинна мати можливість роботи з стандартом X11 через протокол SSH, в тому числі – можливість відтворення графіки через X11

4.3.4.13. Підсистема повинна мати функціонал щодо примусового обмеження файлових операцій (заборону протоколів файлового обміну SFTP та SCP)

4.3.4.14. Результатом контролю привілейованих користувачів що підключаються до цільових систем по протоколу SSH (або X11) повинен бути записаний графічний відеоматеріал (відеоролик)

4.3.4.15. Підсистема повинна мати функціонал експорту збережених графічних відеоматеріалів (відеороликів) в зовнішні відео формати AVI, FLV, MPEG з заданою роздільною здатністю

4.3.4.16. Підсистема повинна забезпечувати контроль привілейованих користувачів що підключаються до цільових систем по протоколу Telnet

4.3.4.17. Підсистема повинна мати можливість роботи з стандартами Telnet 3270 та Telnet 5250

4.3.4.18. Результатом контролю привілейованих користувачів що підключаються до цільових систем по протоколу Telnet (в тому числі - Telnet 3270 та Telnet 5250) повинен бути записаний графічний відеоматеріал (відеоролик) або текстовий журнал дій (команд користувача та відповідей цільової системи на такі команди).

4.3.4.19. Підсистема повинна забезпечувати контроль привілейованих користувачів що підключаються до цільових систем по протоколу VNC

4.3.4.20. Результатом контролю привілейованих користувачів що підключаються до цільових систем по протоколу VNC повинен бути записаний графічний відеоматеріал (відеоролик)

4.3.4.21. Підсистема повинна мати функціонал експорту збережених графічних відеоматеріалів (відеороликів) в зовнішні відео формати AVI, FLV, MPEG з заданою роздільною здатністю

4.3.4.22. Підсистема повинна забезпечувати контроль привілейованих користувачів що підключаються до цільових систем по протоколу HTTP та HTTPS (з підтримкою стандартів SSLv2 та SSLv3)

4.3.4.23. Результатом контролю привілейованих користувачів що підключаються до цільових систем по протоколу HTTP та HTTPS повинен бути записаний текстовий журнал дій (методи передачі даних POST/GET, посилання URL, контент (крім конфіденційних даних), відповіді серверів, дані cookies тощо)

4.3.4.24. Підсистема повинна мати функціонал експорту збережених текстових журналів в зовнішні формати з текстовою структурою

4.3.4.25. Підсистема повинна забезпечувати контроль привілейованих користувачів що підключаються до цільових систем по протоколу ICA (з підтримкою стандартів SSLv2 та SSLv3)

4.3.4.26. Результатом контролю привілейованих користувачів що підключаються до цільових систем по протоколу ICA повинен бути записаний графічний відеоматеріал (відеоролик) або текстовий журнал дій (команд користувача та відповідей цільової системи на такі команди)

4.3.4.27. Підсистема повинна забезпечувати контроль привілейованих користувачів що підключаються до цільових систем по протоколу Citrix StoreFront (з підтримкою стандартів SSLv2 та SSLv3)

4.3.4.28. Результатом контролю привілейованих користувачів що підключаються до цільових систем по протоколу Citrix StoreFront повинен бути записаний графічний відеоматеріал (відеоролик) або текстовий журнал дій (команд користувача та відповідей цільової системи на такі команди)

4.3.4.29. Підсистема повинна забезпечувати контроль привілейованих користувачів що підключаються до цільових систем по протоколу Modbus

4.3.4.30. Результатом контролю привілейованих користувачів що підключаються до цільових систем по протоколу Modbus повинен бути записаний журнал дій (щонайменше - команд користувача)

4.3.4.31. Підсистема повинна забезпечувати контроль привілейованих користувачів що підключаються до цільових систем по протоколу MS SQL (з підтримкою стандартів TDS - Tabular Data Stream)

4.3.4.32. Результатом контролю привілейованих користувачів що підключаються до цільових систем по протоколу MS SQL повинен бути текстовий журнал дій (команд користувача та відповідей цільової системи на такі команди)

4.3.4.33. Підсистема повинна мати функціонал експорту збережених текстових журналів в зовнішні формати з текстовою структурою

4.3.4.34. Підсистема повинна забезпечувати контроль привілейованих користувачів що підключаються до цільових систем по протоколу MySQL

4.3.4.35. Результатом контролю привілейованих користувачів що підключаються до цільових систем по протоколу MySQL повинен бути текстовий журнал дій (команд користувача та відповідей цільової системи на такі команди

4.3.4.36. Підсистема повинна мати функціонал експорту збережених текстових журналів в зовнішні формати з текстовою структурою

4.3.4.37. Підсистема повинна забезпечувати контроль привілейованих користувачів що підключаються до цільових систем по протоколу Oracle

4.3.4.38. Результатом контролю привілейованих користувачів що підключаються до цільових систем по протоколу Oracle повинен бути текстовий журнал дій (команд користувача)

4.3.4.39. Підсистема повинна мати функціонал експорту збережених текстових журналів в зовнішні формати з текстовою структурою

4.3.4.40. Підсистема повинна мати функціонал створення політик щодо команд які вводять привілейовані користувачі під час роботи з цільовими системами. Підсистема повинна підтримувати синтаксис регулярних виразів на базі стандарту POSIX

4.3.4.41. Підсистема повинна мати можливість задавати щонайменше наступних правил під час спрацювання таких політик: блокування користувача, повідомлення відповідальної особи, роз'єднання сесії

4.3.4.42. Підсистема повинна мати функціонал створення політик щодо часових інтервалів в які привілейовані користувачі мають можливість доступу до цільових систем

4.3.4.43. Підсистема повинна мати можливість задавати щонайменше наступних правил для таких політик: дні тижня в які привілейовані користувачі можуть підключатися до цільових систем, часи та хвилини коли привілейовані користувачі можуть підключатися до цільових систем, інтервал дії такої політики (з вказівкою початкових та кінцевих дат та часу), політика розриву активних сеансів по завершення виділеного часу, політика розриву сеансів за причини неактивності користувача протягом певного часу

4.3.4.44. Підсистема повинна мати вбудовані механізми перегляду результатів дій привілейованих користувачів, а саме – перегляд записаних сесій, команд що вводилися та відповідей цільової системи на такі команди. Перегляд результатів повинен забезпечуватися в веб-порталі адміністрування без необхідності встановлення будь-яких засобів (програмних додатків, плагінів тощо)

4.3.4.45. Підсистема повинна мати вбудовані фільтри пошуку результатів дій привілейованих користувачів за різноманітними критеріями, щонайменше за ім'ям привілейованого користувача або користувачів, введеними командами, типом протоколу, ім'ям цільової системи, а також в заданому діапазоні дат. Підсистема повинна мати можливість створення звітів на базі отриманих результатів за заданими фільтрами. Такі звіти повинні мати можливість бути експортовано в вигляді файлів формату CSV, PDF, HTML

4.3.4.46. Підсистема повинна мати функціонал створення політик щодо можливості перегляду окремими привілейованими користувачами паролю(-ей) до цільових систем до яких вони підключаються, в разі якщо такий пароль їм невідомий

4.3.4.47. Підсистема повинна мати вбудовані механізми перегляду таких паролів за будь-який потрібний час (в минулому) в разі якщо вони (паролі) змінювались за допомогою відповідного функціоналу Підсистеми (парольної політики)

4.3.4.48. Підсистема повинна мати функціонал примусового запиту часу доступу та причин підключення до цільової системи привілейованим користувачем з відображенням відповідного поля для відповіді користувача

4.3.4.49. Підсистема повинна мати функціонал додаткового підтвердження (схвалення) підключення до цільової системи привілейованих користувачів відповідальною особою за допомогою веб порталу та мобільного ПЗ

4.3.4.50. Підсистема повинна мати функціонал повідомлень за допомогою каналів електронного зв'язку (email, sms, push тощо) відповідальної особи щодо дії привілейованих користувачів (підключення до цільової системи, відключення від цільової системи, приєднання до сесії іншої особи, спрацювання заданої політики)

4.3.4.51. Підсистема повинна мати функціонал перегляду відповідальними особами сесій привілейованих користувачів в режимі реального часу без будь-якого явного інформування привілейованих користувачів під час такого перегляду

4.3.4.52. Додатково Підсистема повинна надавати відповідальній особі інформацію щодо сесії: ім'я та IP-адресу цільової системи, ім'я привілейованого користувача, тип протоколу що використовується, час початку сесії

4.3.4.53. Підсистема повинна мати функціонал тимчасового або повного примусового припинення роботи сесій привілейованих користувачів відповідальними особами в режимі реального часу

4.3.4.54. Підсистема повинна мати можливість одночасно з припиненням сесії привілейованого користувача блокувати обліковий запис привілейованого користувача сесія якого припиняється

4.3.4.55. Підсистема повинна мати можливість надавати доступ третім особам до сесій привілейованих користувачів які підключені в режимі реального часу так й до сесій що було збережено (записано)

4.3.4.56. Такий доступ повинен надаватися за допомогою унікального URL-посилання з можливістю підключення третьої особи до заданої сесії без будь-якої додаткової авторизації

4.3.4.57. При створенні URL-посилання обов'язкова повинна бути можливість задання часу дії такого посилання та режиму доступу (повний доступ до сесії або доступ тільки в режимі перегляду)

4.3.4.58. Підсистема повинна мати функціонал додавання власних міток (коментарів) до сесій привілейованих користувачів які підключені в режими

4.3.4.59. Підсистема повинна мати функціонал додавання таких міток (коментарів) до будь-якої частини часової шкали з можливістю подальшого пошуку по таким об'єктам

### 4.3.5. Вимоги до підтримки

Підсистема повинна бути доступна для придбання в вигляді віртуального пристрою (VA – virtual appliance)

Виробник Підсистеми повинен надавати вибір Покупцю найбільш оптимальної моделі використання Підсистеми: як у власність (з подальшим придбанням тільки послуг підтримки), так й у тимчасове використання (з можливістю подальшої пролонгації прав на використання Підсистеми).

Виробник повинен дозволяти Покупцю змінювати модель використання Підсистеми після відповідного облікового періоду (закінчення строку дії початково вибраної моделі користування Підсистемою).

Підсистема повинна забезпечуватися сервісною підтримкою не менш ніж 36 місяців в режимі роботи 5x9 (робочі години в робочі дні) на стандартних умовах що пропонує Виробник для даної Підсистеми. Така стандартна підтримка повинна дозволяти безкоштовне вирішення проблем пов'язаних з експлуатацією Підсистеми та безкоштовне оновлення програмного коду (отримання нових версій) до Підсистеми.

Виробник за вимогою Покупця повинен надати можливість придбання розширеної сервісної підтримки з режимом роботи 24x7 (цілодобово) з гарантованими часовими інтервалами реакції та вирішення проблем.

Для вирішення проблем під час експлуатації Підсистеми Виробник повинен надавати електронний сервіс (веб-портал, спеціальну email-адресу, мобільний додаток тощо) для створення заявок від Покупця або його представників з автоматичною реєстрацією таких заявок в системі підтримки Виробника. Такий сервіс повинен мати функціонал підтвердження створення заявок, змін статусу заявок тощо.

Робота с таким сервісом та комунікація з представниками Виробника повинна бути доступна на англійській або російській або українській мові.

Виробник повинен надавати відкритий доступ (без будь-якої попередньої реєстрації) до технічної документації та документації з адміністрування Підсистеми в мережі Інтернет.

Така документація повинна буди доступна на англійській або російській або українській мові.

### 4.4. III. Програмна продукція - Підсистема для фільтрації мережевого трафіку та захисту мережі, аналізу запобігання мережевих вторгнень– 2 комплекти.

Пропонована програмна продукція повинна складатися з серверу управління і збирання логів та двох віртуальних мережевих екранів (Next-Generation Firewall – далі NGFW) з можливістю вияву та попередження загроз (Intrusion Detection / Prevention Systems - IDS/IPS), перевірки файлів на наявність відомого і невідомого шкідливого ПО (Anti-malware / Anti-Virus, Sandbox), вияву і попередженню комунікацій з бот центрами (Anti-bot / Anti-spyware), блокування сучасних атак з використанням DNS-протоколу (DNS Security), контролю доступу до ресурсів Інтернет (URL Fileting), система запобіганню витоку інформації (DLP). Віртуальні мережеві екрани (NGFW) повинні підтримувати відмовостійкість.

#### 4.4.1. Ліцензування

Підсистема має бути ліцензована для роботи протягом 36 місяців.

#### 4.4.2. Вимоги до продуктивності

Максимальна пропускна здатність підсистеми в режимі мережевого екранування із забезпеченням ідентифікації додатків і користувачів (змішаний трафік, appmix) – не менш 5.0 Гбіт/сек для http транзакцій розміром 64 КБ.

Максимальна пропускна здатність підсистеми в режимі попередження і захисту від загроз (Application Control, IPS, Anti-Virus, Anti-spyware чи Anti-bot, Sandboxing, URL filtering,

DNS Security та логування на пристрої) – не менш 3.0 Гбіт/сек. Цей показник повинен бути виміряний з http пакетами та розміром транзакції – 64КБ. Ці дані мають бути опубліковані на офіційному сайті виробника.

Пропускна здатність функціоналу IPsec VPN повинна бути не менше 1.8 Гбіт/сек.

Підсистема повинна підтримувати не менше 2 000 site to site тунелей.

Максимальна кількість нових сесій у секунду – не менш 30 000.

Максимальна кількість підтримуваних сесій – не менш 800 000.

Необхідна кількість використовуваних ядер – 4 ядра процесора (CPU)

### 4.4.3. Вимоги до параметрів розгортання

Кожен віртуальний мережевий екран повинен складатися з двох програмно розділених компонент - компоненти управління пристроєм і компоненти обробки трафіка. Кожна компонента повинна мати свій набір ядер процесора (CPU), оперативної пам'яті (RAM) та інтерфейсів (Ethernet port).

Компоненти управління та обробки трафіку повинні бути незалежні один від одного для того щоб надати можливість керування пристроєм у випадку критичного навантаження трафіком, зокрема під час DoS/DDoS атак.

Вбудована компонента управління повинна бути керована за допомогою веб інтерфейсу з можливістю налаштування політик безпеки та мережевих конфігурацій з єдиної веб консолі без необхідності встановлення додаткових програм на ПК.

Порт управління (Management port) повинен бути програмно ізольований від мережевих портів для обробки трафіку.

### 4.4.4. Вимоги до підтримуваних протоколів і режимів функціонування

Підтримка статичної маршрутизації IPv4/IPv6 та протоколів динамічної маршрутизації BGPv4, OSPFv2/v3, RIP v2. Якщо цей функціонал потребує ліцензії, вона повинна бути включена в пропозицію.

Підтримка роботи мережевих інтерфейсів у режимах прослуховування «дублюючого» трафіка з Span-Портів комутаційного устаткування, що підключається, у прозорому режимі без зміни MAC і IP-Адрес (Virtual Wire), у режимі комутації трафіка (Layer 2), у режимі маршрутизації трафіка (Layer 3).

Підтримка одночасної роботи різних мережевих інтерфейсів у будь-яких перерахованих режимах у будь-якій комбінації без обмежень в рамках одного віртуального мережевого екрану.

Підтримка зміни режиму функціонування портів (Layer 2, Layer 3, прозорий режим та режим прослуховування) без необхідності перезавантажувати Підсистему.

Підсистема повинна вміти працювати в режимі комутатора (тобто мати можливість виділити більше 2х портів для роботи в режимі комутатора).

Підсистема повинна вміти здійснювати VLAN трансляцію на L2 рівні між підмережами.

Підтримка Static та Dynamic (Hide) NAT.

Підтримка NAT у прозорому режимі.

Підтримка IPV6, включаючи ідентифікацію додатків і користувачів.

Підтримка multicast маршрутизації і протоколів – PIM-SM, PIM-SSM, IGMP v1, v2, v3.

Підтримка маршрутизації між VLAN, організованими на мережевому екрані.

Підсистема повинна підтримувати не менше 4000 vlan.

Підтримка функціонала трансляції адрес NAT, сервера DHCP і DHCP relay.

Підтримка тегування фреймів по 802.1.

Підтримка агрегування інтерфейсів по 802.3ad (підтримка LACP).

Підтримка передачі більших пакетів (Jumbo frames).

Підтримка SNMPv3.

Підтримка Netflow. Netflow профіль повинен визначатися на основі фізичних портів.

Підтримка протоколу LLDP (Link Layer Discovery Protocol). Таким чином, Підсистема повинна мати можливість подавати інформацію про інші пристрої (адреса MAC, ім'я системи, підключений до нього порт).

Підтримка політик Policy Based Forwarding для IPv4 та IPv6 протоколів.

Підтримка BFD (Bidirectional Forward detection). Це дозволить швидше адаптуватися до будь-яких змін на рівні маршрутизації.

Підтримка віртуальних маршрутизаторів – не менш 10 шт.

Підтримка зон безпеки – не менш 40 шт.

Підтримка site-to-site та client-to-site IPsec VPN.

Число максимально можливих Client SSL VPN – не менше 2 000.

Число максимально можливих Clientless VPN – не менше 400.

Число IPSEC VPN тунелів (Site to site) – не менше 2 000.

Число одночасних сеансів розшифрування SSL – не менш 15 000

Підтримка перевірки загроз та перевірка вмісту тунельних протоколів: GRE до 2 рівнів, GTP-U, нешифрованих IPSEC: ESP-null або AH.

### 4.4.5. Вимоги до відмовостійкості

Підтримка побудови відмовостійкого кластеру високої доступності High-Availability (HA) – Active/Passive та одночасної роботи обох міжмережевих екранів кластеру в активному режимі – Active/Active

Для переключення між компонентами кластеру повинен здійснюватися моніторинг інтерфейсів (interface monitoring) та шляху до вказаних ресурсів (path monitoring)

### 4.4.6. Вимоги до функціоналу Підсистеми

Підсистема повинна контролювати стан сесій (Stateful inspection) з фільтрацією пакетів та ідентифікацією застосунків.

Підсистема повинна бути зонним мережевим екраном (Zone-based). Один або більше інтерфейсів або суб інтерфейсів можуть належати одній зоні. Політики доступу (firewall rules) та політики NAT повинні бути засновані на зонах.

Політики NAT повинні мати свій набір правил, незалежно від політик доступу (firewall rules).

Розпізнавання і блокування мережевих додатків на сьомому рівні моделі OSI по трафіку, що проходить через мережевий екран, у тому числі індивідуально для всіх додатків, що використовують загальний порт, у тому числі 80 і 443, що й використовують динамічні TCP/ UDP-Порти;

Управління додатками повинно показувати залежності додатку, щоб мати можливість будувати білі списки без помилок.

Розпізнавання трафіку що інспектується на Layer-7 моделі OSI по сигнатурах, наступного програмного забезпечення (додатків), протоколів або сервісів:

• Сервісів автентифікації, включаючи Microsoft Active Directory, LDAP, RADIUS, TACACS+, Kerberos, SAML, Syslog Monitoring/Parser (Підсистема повинна підтримувати зіставлення user-to-ip, обробляючи повідомлення від Syslog);

• СУБД, включаючи Microsoft SQL, Oracle, тощо;

• Файлові сервіси, включаючи Microsoft SMB;

• Систем електронного документообігу й обміну повідомленнями, у тому числі Microsoft Sharepoint, Exchange, Office 365, Google Docs;

• Протоколів обміну електронною поштою: SMTP, POP3, IMAP;

• Протоколів VOIP і аудіо-відео-конференцій, включаючи SIP, H.323, H.245, H.225, Webex;

• Сервісів відновлення програмного забезпечення, включаючи Microsoft Update, антивірусного ПО, Adobe, Java;

• Сервісів резервного копіювання;

• Сервісів віртуалізації й термінального доступу, включаючи Vmware, Microsoft RDP;

• Протоколів дистанційного доступу, включаючи Telnet, SSH, VNC, Radmin;

• Мережеві протоколи, включаючи протоколи динамічної маршрутизації й SSL, IPSec VPN;

• Електронної пошти;

• Соціальних мереж;

• Засобів миттєвого обміну повідомленнями;

• Засобів аудіо-відео-конференцій;

• Потокового аудіо-відео (незалежно від веб-сайту), аудіо й відео по HTTP;

• Засобів публікації робочого стола й надання дистанційного доступу, включаючи Team-Viewer;

• Зовнішніх проксі-серверів й анонімайзерів, включаючи Tor, Ultrasurf, Freegate, SOCKS, PHP Proxy;

• Засобів побудови VPN і тунелів поверх інших додатків, включаючи Freenet, Open-vpn, Vtun, Rdp-to-Tcp, Tcp-over-Dns

Рішення повинно підтримувати режим "Безпечний пошук" для YouTube та CIPA-сумісного пошуку Google (Рішення не повинно працювати в режимі проксі).

Надання вбудованих у мережевому екрані засобів створення власних сигнатур додатків по регулярним вираженням з використанням декодерів HTTP(S), FTP, SMB, SMTP, RPC і ін., а також по масці для вмісту TCP/ UDP-Пакетів;

Розпізнавання мережевих додатків по зашифрованому SSL (підтримка ключів RSA до 2048 біт) і SSHv2 трафіку, що проходить через мережевий екран (дешифрація SSL, SSHv2), - як для вхідних, так і для вихідних підключень, прозоро для користувачів у домені, з можливістю контролю окремих функцій додатків, включаючи відправлення повідомлень у соціальних мережах, файловий обмін, потокове аудіо, відео;

Послідовне розпізнавання різних додатків, використовуваних у рамках однієї сесії;

Правила контролю доступу повинні підтримувати можливість враховувати час, день, дата та період надання такого доступу.

Розпізнавання користувачів, що використовують мережеві додатки, за рахунок інтеграції з корпоративними сервісами аутентифікації користувачів, такими як Microsoft Active Directory, Microsoft Exchange, LDAP, Novell eDirectory;

Можливість створення правил на основі груп користувачів та окремих користувачів. Підсистема повинна зберігати інформацію про користувачів у відповідних логах.

Інтеграція з Microsoft Active Directory, повинна здійснюватися без змін в Active Directory та не повинна використовувати обліковий запис адміністратора Active Directory домену.

Можливість інтеграції з іншими сервісами аутентифікації (наприклад, контролерами бездротових мереж) через відкритий XML API;

Можливість створення користувач-ай-пі меппінгу (user-IP mapping) завдяки парсингу syslog повідомлень відправлених системою що автентифікувала користувачів.

Можливість створювати та використовувати у правилах динамічні групи користувачів. Динамічні групи користувачів дозволяють “на льоту” видаляти користувача з групи (додавати користувача в групу) без необхідності змін у відповідній директорії (наприклад Active Directory) та без необхідності встановлювати політики. Це дає можливість уповноваженим

адміністраторам або зовнішнім систем видаляти користувача з динамічної групи користувачів, наприклад у випадку компрометації відповідного користувача.

Створення правил у єдиній політиці безпеки, використовуючи в якості класифікаторів дані про IP-адреса відправника, одержувача, використовуваних сервісів (TCP/UDP-Портів), імена користувачів, груп користувачів і використовуваних користувачем або групою користувачів додатків або певних категорій додатків.

У створюваних політиках повинна бути можливість реалізації наступних дій:

• Дозволу або заборони;

• Дозволу конкретному додатку або категорії додатків використовувати тільки стандартні або строго певні TCP/ UDP-Порти. При цьому ці порти не повинні бути використані іншими додатками без політики, що дозволяє такі взаємодії в явному виді;

• Дозволу або заборони, заснованого на розкладі, користувачі або групі користувачів;

• Застосувати маркування DSCP і обмеження по трафіку, використовуючи політики QOS на основі додатків, IP-адрес, DSCP, користувачів і груп користувачів;

• Реалізація QOS для трафіка real-time, ідентифікованого на рівні додатків;

• Можливість перемаркування QoS на основі адреси джерела/призначення, порту, L7 застосунку

• Можливість застосовувати перенаправлення трафіка на основі політик (Policy Based Forwarding) на основі IP адреси (source та/або destination), користувача, застосунку або URL;

• Можливість маршрутизації трафіку різних застосунків по різних маршрутам передачі даних

• Можливість маршрутизації трафіку різних URL-запитів по різних маршрутам передачі даних

• Можливість заборони окремого функціоналу у додатках;

• Можливість використовувати будь-яку комбінацію з вищенаведених дій;

• Можливість побудови whitelist/blacklist політики для окремо взятих користувачів.

Інспекція змісту трафіка протоколів:

• Generic Routing Encapsulation.

• Non-encrypted IPsec traffic (NULL Encryption Algorithm for IPsec and transport mode AH IPsec).

Підсистема повинна мати базовий DLP функціонал з налаштуванням через графічний інтерфейс з можливістю пошуку заданої інформації через регулярні вирази, попередньо-налаштовані шаблони або властивостей файлів (відповідна ліцензія повинна бути додана у пропозицію).

Підсистема повинна забезпечувати функціонал оптимізації політик, зокрема на основі використання додатків; виявлення та видалення невикористаних правил політики.

Для створення більш суворих правил та оптимізації політики в інтерфейсі управління на Підсистемі повинні бути доступні наступні функції:

• Повідомляти про правила з невизначеними застосунками/додатками, ідентифікувати додатки що проходять через ці правила, та активувати їх у правилі, вибравши потрібні з перелічених додатків.

• Повідомляти про додатки, які визначені та не використовуються в правилах. Про невикористані підписи заявки можна повідомити за останні 7, 15, 30 днів.

• Повідомляти інформацію про першу та останню дату ідентифікації додатку, який ідентифікувалися в правилі, та скільки пропускної здатності він спожив за останні 30 днів.

• Ідентифікувати правила, які не використовувались протягом останніх 30 днів і 90 днів.

Правила безпеки можуть застосовуватися відповідно до географічних регіонів; до правила можна додати кілька географічних регіонів

Обмеження пропускної здатності може застосовуватися на основі імені користувача / групи, IP-адреси цілі / джерела та програми.

Можливість автоматично блокувати трафік з певних джерел окремою частиною мережевого екрана, до того, як ці пакети будуть використовувати ресурси основного процесора або буфера пакетів віртуального NGFW.

Наявність сервісу сканування нових потенційно шкідливих файлів у середовищі Microsoft Windows, включаючи файли, що виконуються (у тому числі EXE, DLL, SCR, BAT, і ін.), передані по мережі, у поштових повідомленнях SMTP/POP3, включаючи шифровані повідомлення за допомогою SSLз, що забезпечує, поведінки підозрілих файлів і посилань у приватній або зовнішній хмарі («пісочниці»), виявлення нового шкідливого ПО й автоматичну генерацію антивірусної сигнатури протягом 24 годин і оновлення репутаційної бази URL протягом 30 хв.

Мати розвинені функції візуалізації: візуалізація в простому та зручному форматі, активності мережевих додатків, виявлених і блокованих мережевих загроз додатків, що використовують користувачі. Можливість фільтрації інформації, використовуючи різні фільтри (по додатках, по погрозах, по користувачах, IP-адресам, TCP/ UDP-Портам, зонам безпеки, типам погроз і ін.);

Мати можливість створення звітів. Мережевий екран повинен мати функції по автоматичній генерації звітів і звітів за розкладом по різних тематичних функціях по ручному налаштуванню створюваних звітів. Повинна бути можливість перегляду звітів як безпосередньо через графічний веб-інтерфейс керування (GUI) мережевим екраном, так і можливість експортування звітів у формати PDF і CSV;

Мати можливість інтеграції з підсистемою централізованого керування, логування, звітності, відновлення програмного забезпечення мережевих екранів того ж виробника;

Мати можливість буферизації логів локально на виділений дисковий простір віртуальної машини у випадку короткочасної недоступності підсистеми централізованого логування;

Мати можливість інтеграції з SIEM-Системами різних виробників по протоколу Syslog із забезпеченням гнучкого налаштування формату логів;

Мати рольове керування доступом локальних адміністраторів:

• Можливість обмежити область перегляду й керування на рівні віртуального пристрою в цілому, а також окремих віртуальних систем (контекстів);

• Можливість надати доступ у режимі виправлення або тільки для читання, або заборонити доступ до будь-якого розділу веб-інтерфейсу мережевого екрану;

• Можливість надати доступ у режимі виправлення або тільки для читання, або заборонити доступ до CLI мережевого екрану;

Мати наявність єдиного інтерфейсу керування для керування політиками безпеки, профілями та налаштуваннями пристроїв та мереж, без спеціальних пристроїв керування

Керування політиками безпеки та мережевими налаштуваннями повинне здійснюватися по протоколах HTTPS і SSH без необхідності установки якого-небудь додаткового ПО керування на робочу станцію адміністратора та без використання хмарних серверів управління;

Інтерфейс керування мережевими екранами (веб і CLI) повинен бути уніфікований з підсистемою централізованого керування, логування, звітності, відновлення програмного забезпечення;

Підтримка міток Cisco TrustSec SGT Tag;

Підтримка функціоналу динамічних адресгруп (Dynamic Address Group) та динамічних груп користувачів (Dynamic User Group), що дозволяє динамічно, за допомогою XML API, оновлювати такі групи в правилах безпеки без необхідності встановлювати політики безпеки.

Підсистема повинна мати можливість виконувати розшифрування SSL/TLS та SSH. Підтримка розшифрування протоколів TLS 1.0, TLS 1.1, TLS 1.2 та TLS 1.3

Підсистема повинна мати можливість перевіряти трафік HTTPS та застосовувати IPS, контроль додатків, фільтрування URL-адрес та антивірусні засоби захисту.

Підсистема повинна здійснювати розшифрування HTTPS у вхідному (inbound) та вихідному (outbound) напрямках.

Підсистема повинна підтримувати інтеграцію з HSM (hardware security module) для управління цифровими ключами.

Підтримка інспекції тунелів VxLAN

Підсистема повинна мати можливість застосовувати IPS, Application Control та Anti-virus, досліджуючи трафік HTTPS.

Підсистема повинна проводити перевірку HTTPS у вхідному та вихідному напрямку.

Правила інспектування (дешифрування) трафіку HTTPS повинні створюватися на основі імені користувача / групи користувачів, джерела IP (source IP) / мережі / зони, цільового IP (destination IP) / Цільової мережі / Цільової зони та категорії URL.

Підсистема повинна надавати можливість створювати правила виключення дешифрування у випадках, коли вміст трафіку HTTPS не слід бачити (банківські операції тощо).

Повинна бути можливість перевіряти сертифікат HTTPS сесій та запобігати сесії із закінченими, ненадійними або відкликаними сертифікатами.

Підсистема повинна вміти дешифрувати SSL веб трафік і відправляти копію дешифрованого трафіку на зовнішні пристрої аналітики, використовуючи функціонал дзеркалювання трафіка. Відповідна ліцензія повинна бути додана в пропозицію.

Підсистема повинна мати можливість розшифровувати на ньому клієнтський веб-трафік SSL/TLS та надсилати цей розшифровувати трафік стороннім пристроям або системам обробки даних трафіку (IPS, Network Forensic тощо). Сторонні пристрої або системи, про які йдеться, повинні бути в змозі забезпечити продовження проходження трафіку шляхом відправки цього трафіку назад на Підсистему і знову зашифрувати його після виконання необхідних операцій над трафіком.

Підсистема повинна мати можливість дзеркалювати та пересилати UDP/TCP трафік на сторонні інструменти аналітики для інспекції цього трафіку та повернення його назад для подальшої передачі клієнту та/або серверу

Підсистема повинна мати можливість застосовувати правила безпеки у відповідності до географічної зони, з можливістю створення одного правила з декількома географічними зонами.

### 4.4.7. Вимоги до можливостей запобігання вторгнень, розпізнавання й блокування шкідливого або забороненого трафіка в Підсистемі

Підсистема повинна мати архітектурну перевірку, фільтрацію пакетів IP та функції розпізнавання додатків

Підсистема повинна мати такі служби безпеки:

• Брандмауер наступного покоління (NGFW)

• IPSEC VPN, SSL VPN

• Контроль додатків (Application Control)

• Антивірус (Antivirus/Antimalware)

• Запобігання вторгненням (IPS)

• Антишпигунську (antispyware/antibot)

• Блокування атак з використанням DNS протоколу (DNS Security)

• Фільтрація URL посилань (URL filtering)

• Аналітика мережевого трафіку (NTA)

• Інтеграція з каталогами для ідентифікації користувачів (Identity Awareness)

• Безпечний віддалений доступ (Remote Access VPN) з перевіркою віддаленого хоста на відповідність вимогам (compliance check)

• Можливість інспекції переданого через мережевий екран умісту трафіка в реальному режимі часу в потоці по сигнатурах і поведінці, захист від вразливостей, мережевих атак і

шкідливого програмного забезпечення, розпізнавання типів файлів по їхнім сигнатурам, визначення вірусів, переданих по веб, через електронну пошту, FTP, SMB, шпигунського програмного забезпечення, мережевих «worms», блокування передачі певного вмісту з використанням регулярних виразів, у тому числі для додатків, що використовують шифрування SSL і SSHv2;

• Антивірусний захист, захист від шпигунського програмного забезпечення, захист від вразливостей і мережевих атак (система виявлення й запобігання вторгнень), URL-Фільтрація з використанням динамічної репутаційної бази, що підтримує категоризацію для різних розділів того самого веб-сайту, включаючи підтримку категорій для веб-сайтів на різних мовах, блокування передачі файлів по типах, певних сигнатур;

• Можливість використання додаткових функцій сканування нових потенційних шкідливих файлів у середовищі Microsoft і Android, включаючи файли, що виконуються ( у тому числі EXE, DLL, SCR, BAT, і ін.), документи форматів PDF (перевірка на різних версіях Adobe Reader), MS Office 2003, 2007 і вище, Java і Flash, Android APK, посилання http:// і https:// виявлення нового шкідливого програмного забезпечення й автоматичну генерацію антивірусної сигнатури в режимі реального часу;

• Автоматична кореляція логів різного типу (мережеве екранування, захист від погроз, контроль передачі файлів, URL-Фільтрація), згенерованих у рамках однієї сесії.

Підсистема повинна мати наступні функції системи протидії вторгнень (IPS):

• Можливість створення різних політик IPS для різних користувачів або груп користувачів.

• Можливість пошуку IPS сигнатур на пристрої за допомогою CVE, рівнів критичності та типу хосту (клієнт/сервер).

• Можливість індивідуального налаштування сигнатур IPS системи реагувати на атаки наступним чином: Allow, Alert, Deny, reset-both, reset-client, reset-server, Block-IP. Блокування на основі IP повинно бути виконуватися на основі source IP та одночасно source та destination IP.

• Фільтри IPS, які використовуються для протидії атакам, повинні бути в змозі оновлюватися з файлу оновлення або через Інтернет. Крім того, за необхідності оновлення сигнатур повинно робитися автоматично без втручання користувача.

• Запропоноване функціональність IPS повинна включати технологію детектування аномалій в використовуваних аномаліях (Protocol Anomaly Detection) які дозволяють блокувати атаки, не спираючись на наявні сигнатури.

Функціональність IPS повинна бути в змозі протистояти наступним атакам:

• Brute Force

• Code/Command execution

• Sql-injection

• Exploit-kit

• Denial of Service

• Info-leak

• Overflow

• Scan

Підсистема повинна мати функціональність Anti-Spyware/Anti-bot для виявлення та блокування

Функціональність Anti-Spyware/Anti-bot повинна мати наступні можливості:

• працювати незалежно від порту і протоколу і повинен перевіряти весь IP трафік в Інтернет.

• виявляти запити на визначення (resolution requests) IP адрес командних центрів ботнетів (Botnet command and control centers) і блокувати їх через ДНС запити

• функціонал DNS Sinkhole у випадку запиту шкідливого доменного імені повинен видавати IP address призначену адміністратором (таким чином інфіковані системи зможуть бути легко ідентифіковані)

• функціонал блокування відомих ботнетів за допомогою сигнатур. Система повинна надавати можливість адміністратору налаштовувати ботнет сигнатури

• для дій сигнатур повинні бути доступні наступні дії:

Allow, Alert, Deny, reset-both, reset-client, reset-server, Block-ip

• різні політики Anti-spyware повинні створюватися для різних користувачів і груп користувачів.

Функціональність Anti-spyware повинна включати ідентифікацію та блокування наступних атак:

• adware

• Botnets

• Backdoor

• Browser-Hijacker

• Data-theft

• keylogger

• spyware

• net-worm

• p2p-communication

Підсистема повинна мати Anti-Virus функціонал для виявлення і попередження з наступними можливостями:

• Блокування відомого шкідливого ПО на основі сигнатур

• Повинна мати можливість потокового сканування. Повинна сканувати архівні файли

• Архітектура Anti-virus повинна мати можливість інтегруватися з Active Directory таким чином що б правила Anti-virus могли бути визначені на основі користувача чи групи користувачів в Active Directory

• Можливість виключити антивірусні сигнатури із бази даних сигнатур (можливість задавати виключення)

• Різні політики Anti-virus повинні створюватися для різних користувачів і груп користувачів

• Anti-virus повинен блокувати шкідливі файли, передані через протоколи FTP, HTTP, SMB, POP3

Запропонована Підсистема повинна мати функціонал захисту від атак нульового дня за допомогою сканування файлів що передаються у трафіку

Вимоги до функціоналу захисту від атак нульового дня

• Підсистема повинна використовувати додаткову локальну або хмарну пісочницю (sandbox) для аналізу файлів

• Підсистема повинна бути здатним відправляти підозрілі файли (наступні формати файлів повинні підтримуватися: 7-ZIP, RAR, ZIP, Adobe Flash, APK, JAR, PDF, MS-Office DOC, DOCX, RTF, XLS, XLSX, PPT, PPTX, .exe, .dll, а також лінки в пошті, ELF формат файлів ОС Linux, формати файлів Mach-O, DMG, та PKG операційної системи Mac OS X) в пісочницю локальну або хмарну пісочницю

• Підсистема повинна мати можливість отримувати відповідні оновлення в режимі реального часу для забезпечення захисту від шкідливих файлів із локальної або хмарної пісочниці

• Пристрій повинен мати можливість ідентифікувати та блокувати в режимі реального часу невідомі шкідливі портативні виконувані файл та скрипти PowerShell за допомогою алгоритмів машинного навчання, оцінюючи деталі файлу, включаючи поля та шаблони декодера. Цей рівень захисту повинен забезпечувати розширене охоплення файлів, сигнатури для яких ще не існують

• Запропоноване рішення повинно ідентифікувати користувачів, які завантажували шкідливі файли

Підсистема повинна мати функціонал DNS Security протидії атакам із зловмисним використанням протоколу DNS

Функціонал DNS Security повинен включати в себе наступні можливості:

• Аналіз підозрілих DNS-Запитів і локалізація заражених станцій за допомогою технології DNS sinkhole (підміна відповіді DNS-Сервера)

• Блокування відомих зловмисних доменних імен за допомогою репутаційних баз

• Функціонал повинен використовувати алгоритми машинного навчання в хмарі для ідентифікації потенційно шкідливих доменних імен

• Виявлення та блокування DNS-тунелів (DNS tunneling) за допомогою машинного навчання, що аналізує якість та поведінку DNS-запитів (частота запитів, ентропію тощо)

• Повинен здійснюватися аналіз та виявлення DGA (domain generation algorithm) та Dictionary DGA, тобто визначення чи домен згенерований машиною, а не людиною, шляхом реверсивної інженерії та аналізу інших часто використовуваних методів. У випадку виявлення що домен створений DGA алгоритмом він може бути заблокований

Функціонал DNS Security повинен вміти виявляти низку інших типів атак таких як:

ultra-slow DNS tunneling

dangling DNS

NSNX DDoS attacks

fast-flux domains

DNS rebinding

виявлення нових зареєстрованих доменів (NRD);

Підсистема повинна мати функціонал URL-фільтрації

Можливості підсистеми URL-фільтрації

• Функція фільтрації URL-адрес повинна працювати в інтеграції з Active Directory, завдяки чому правила фільтрації URL-адрес можуть бути визначені на основі користувачів та груп користувачів, визначених в Active Directory

• Наявність та можливість змінювати портал блокування та попередження відвідування неприйнятних URL-адрес

• Можливість динамічно оновлювати списки C&C (Command and Control) та сайтів що містять шкідливе програмного забезпечення

• Функція фільтрації URL-адрес повинна мати функцію XFF (X-forwarded-for)

• Можливість написання політик обмеження пропускної здатності для категорій URL-адрес

• Можливість класифікувати URL-адреси як високо-ризиковані (шкідлива активність, пов’язана з URL-адресами за останні 30 днів), так і URL-адреси із середнім ризиком (шкідлива діяльність, пов’язана з URL-адресою за останні 60 днів)

• Можливість класифікувати URL-адреси, зареєстровані за останні 30 днів (нові зареєстровані домени)

• Можливість зберігати та передавати детальні журнали URL-адрес, до яких здійснюється доступ у зовнішні системи через syslog

Функціонал URL-фільтрації повинен мати можливість застосовувати машинне навчання на веб-сторінках, щоб запобігти потраплянню шкідливих варіантів експлойтів JavaScript та фішингу у мережу. Цей функціонала машинного навчання повинен динамічно аналізувати та виявляти шкідливий вміст, оцінюючи різні деталі веб-сторінок, використовуючи ряд моделей машинного навчання в режимі реального часу.

Функціонал URL-фільтрації повинен використовувати хмарну технологію перевірки веб-трафіку на основі Машинного Навчання (ML) у режимі реального часу та мати можливість виявлення та запобігання невідомим розширеним безфайловим веб-атакам, включаючи цільовий фішинг, зловмисне програмне забезпечення, що доставляється через Інтернет а також експлойти, соціальну інженерії та інші види веб-атак.

Підсистема повинна мати функціонал захисту від фішингових атак за допомогою функції контролю ідентичності користувача. Запропоноване рішення повинно мати можливість запобігти надсиланню/викраденню інформації про користувача (логіну) та паролю на рівні HTTP / HTTPS POST. Він повинен мати можливість контролювати облікові дані користувачів в інтеграції з Active Directory. Відповідна ліцензія повинна бути включене в запропоноване рішення.

Підсистема повинна мати функціонал фільтрації даних (Data filtering) і працювати використовуючи правила. Ідентифікація типу файлу повинна здійснюватися за допомогою ключових слів регулярних виразів. Ліцензії, необхідні для цього, повинні бути включені в пропозицію.

Підсистема повинна мати функціонал віддаленого безпечного підключення (Remote Access VPN)

Можливості віддаленого безпечного підключення (Remote Access VPN)

• VPN клієнт повинен підтримати наступні ОС: Windows, MacOS, Android, Apple iOS

• Пристрій повинен підтримувати також безклієнтний доступ до ресурсів компанії (SSL VPN)

• VPN клієнт повинен вміти працювати, використовуючи протокол IPSec, та мати можливість переключення на SSL/TLS

• VPN клієнт повинен підтримувати аутентифікацію за допомогою сертифіката, включаючи попередню аутентифікацію (pre-logon) за допомогою машинного сертифікату

• Пристрій повинен підтримувати логін користувача завжди увімкнений (always on), на вимогу (on demand), попередній вхід (pre-logon)

• VPN клієнт повинен підтримувати аутентифікацію за допомогою SAML, Kerberos, Radius, клієнтський сертифікат, локальну базу даних та LDAP каталог

• VPN клієнт повинен підтримувати функцію роздільного тунелювання для додатку (процесу), маршруту та домену

• VPN клієнт повинен підтримувати функціональність профілів віддаленої перевірки хоста на відповідність заданим вимогам

• Профілі віддаленої перевірки хоста повинні включати: перевірки версії ОС, контроль встановлених патчів

• Профілі перевірки віддаленого хоста повинні включати: перевірку на наявність зазначеного антивірусу, наявності шифрування, наявності резервної копії, DLP агенту, та/або корпоративного сертифікату

• Профілі перевірки віддаленого хоста повинні включати в себе кастомізовані перевірки: наявність процесів і значень реєстру/plist

• Міжмережевий екран повинен вміти будувати політики безпеки на основі відповідності профілям перевірки віддаленого хоста

### 4.4.8. Додаткові обов'язкові вимоги до NGFW

Більше одного адміністратора може одночасно змінювати конфігурацію пристрою.

Зміни правил повинні бути активними після проведення операції "Встановити". Операція "встановити" повинна мати опцію - встановити зміни зроблені всіма адміністраторами або вибрати зміни якого адміністратора потрібно застосувати.

У кожній операції завантаження правил пристрій може автоматично зробити резервну копію конфігурації.

Підсистема повинна мати функцію управління правилами для запобігання конфлікту правил у своєму веб-інтерфейсі управління. Система має попереджати адміністратора, якщо правило буде дублюватися чи затінятися існуючими правилами.

Журнали можуть надсилатися до зовнішніх систем управління журналом через SNMP, syslog.

Журнали повинні зберігатися локально. Також повинна існувати опція надсилати журнали до центральної системи управління, якщо така буде встановлена.

Підсистема повинна мати можливість надсилати журнали за допомогою snmp, syslog з можливістю використання спеціально визначених фільтрів.

Підсистема повинна підтримувати створення зовнішніх динамічних списків блокування IP / URL / домену. Пристрій повинен отримувати доступ до цього списку по HTTP протоколу. При внесенні змін в цей список пристрій повинен автоматично заблокувати (або дозволити - в залежності від встановленої політики) ці IP / URL / домени без необхідності встановлювати (застосувати) політики на самому пристрої. Ємність списків повинен включати в себе не менше ніж 50 000 IP, 100 000 URL та не менше ніж 500 000 доменних імен.

Підтримка динамічних списків блокування для зовнішніх джерел ThreatIntelligence

Перелік шкідливих IP-адрес, виявлених виробником у службі кібер-розвідки, повинно постійно оновлюватися на пристрої. Таким чином, доступ до цих ІС може бути заблокований.

Підсистема повинна мати опцію налаштування порогової кількості одночасних сесій для протистояння SYN Flood, UDP Flood, ICMP Flood.

Підсистема повинна вміти ідентифікувати заблокувати сканування портів: TCP port scan, UDP Ports scan та sweep scan.

Резервні правила повинні відновлюватися та активуватися без необхідності перезавантаження.

NGFW повинно бути побудовано на моделі безпеки із застосуванням білого списку, а не чорного списку та мати просту модель управління політиками. Керування за допомогою простих графічних інструментів та редактора політик, що об'єднує налаштування програм, користувачів та контенту разом.

Всі сервіси, що використовуються NGFW мають можливість отримувати оновлення ПЗ та сигнатур безпеки (а саме - Application Control, IPS, Antivirus, Antispyware, DNS Security, SSL Decryption, URL filtering, Data Filtering, Sandbox) протягом не менш ніж 36 місяців з дня активації NGFW.

### 4.4.9. Вимоги до системи керування Програмними комплексами мережевої безпеки

Вимоги до системи централізованого управління, логування, звітності та оновлення програмного забезпечення (надалі - Системи централізованого управління) програмних та програмних мережевих екранів:

• Підтримка всіх моделей і версій ПО мережевих екранів того ж самого виробника, що й програмних та програмно-апаратних мережевих екранів;

• Уніфікація веб-інтерфейсу з NGFW того ж виробника - аналогічні управління керування, розділи, закладки та графічне оформлення;

• Уніфікація CLI с NGFW того ж виробника – аналогічні команди;

• Можливість із веб-інтерфейсу Системи централізованого управління перемикатися в веб-інтерфейс управління конкретним NGFW і назад;

• Система повинна постачатися у вигляді віртуальної машини та підтримувати наступні гіпервізори: VMware ESXi 6.0, 6.6 та 6.7; Hyper-V - Windows Server 2016 з Hyper-V роллю та Hyper-V 2016;

Ліцензія для Системи централізованого управління повинна дозволяти керувати 2 (двома) віртуальними пристроями NGFW, та працювати в якості окремого лог колектора

Вимоги до функцій централізованого управління:

• Можливість об'єднання керованих NGFW в групи - як фізичних пристроїв, так і окремих віртуальних систем (контекстів);

• Можливість застосування єдиних налаштувань інформаційної безпеки і тиражування налаштувань мережевих і системних параметрів з подальшим коригуванням для врахування локальних особливостей;

• Можливість застосування до груп пристроїв централізованих налаштувань об'єктів

Можливісті застосування до груп пристроїв централізованих налаштувань об'єктів

• Адресних об'єктів (IP-адреси, FQDN) і груп;

• Створених вбудованими засобами NGFW сигнатур додатків і загроз;

• Статичних і динамічних груп додатків;

• Створених категорій URL;

• Профілів настройки динамічної URL-фільтрації, системи виявлення та запобігання вторгнень (IDS / IPS), антивірусного захисту, захисту від шпигунського ПЗ (в тому числі ботнетів) і DoS-атак;

• Профілів відправки логів;

• Розклад дії політик;

Можливість застосування до груп пристроїв централізованих налаштувань політик:

• Інформаційної безпеки (міжмережевого екранування і захисту від загроз);

• Дешифрування SSL і SSHv2;

• QoS;

• Перевизначення додатків;

• Захисту від DoS-атак;

Можливість вибіркового застосування політик до окремих пристроїв в групі, а також до всіх, крім окремих.

Можливість комбінування централізовано налаштованих і локальних політик на Підсистемі. При цьому централізовано налаштовані політики і об'єкти повинні бути доступні локальному адміністратору в режимі «тільки для читання».

Можливість застосування до груп пристроїв шаблонів конфігурації всіх мережевих і системних параметрів

, в тому числі:

• Створення віртуальних систем (контекстів) - за умови підтримки з боку NGFW;

• Налаштування ролей адміністраторів;

• Налаштування ідентифікації і аутентифікації користувачів;

• Налаштування зон безпеки, параметрів мережевих інтерфейсів (тип, IP-адресація), маршрутизації, VLAN, IPsec / SSL VPN, QoS;

• Налаштування захисту зон МЕ від атак L3-L4, включаючи flood, сканування мережі та модифікацію заголовків TCP / UDP;

Надання можливості локального адміністратора вибірково скорегувати мережеві і системні параметри після централізованого застосування шаблонів.

Прийом і зберігання логів в форматі NGFW того ж виробник.

Підтримка двох-рівневої системи логування та звітності:

• Роль сервера логування - зберігання логів від підключених МЕ і генерація фрагментів звітів на їх основі;

• Роль сервера управління - централізоване конфігурування і генерація звітів на основі балок, збережених розподілений на серверах логування, агрегування звітності;

• Можливість суміщення ролей сервера управління і логування на одному пристрої;

Візуалізація трафіку і загроз, ідентична окремому NGFW, але на основі агрегованих логів і статистики.

Можливість побудови всіх типів звітів, ідентично окремому NGFW, але на основі агрегованих логів і статистики.

Можливість централізованого оновлення ПЗ для кожної моделі керованих NGFW.

Можливість централізованого оновлення сигнатур додатків і загроз.

Можливість централізованого контролю наявності та актуальності ліцензій, підписок і контрактів технічної підтримки виробника.

Рольове управління доступом адміністраторів

, в тому числі:

• Можливість обмежити область перегляду і управління на рівні груп керованих МЕ, а також окремих пристроїв;

• Можливість надати доступ в режимі редагування або тільки для читання, або заборонити доступ до будь-якого розділу веб-інтерфейсу ПЗ управління, логування, звітності та оновлення;

• Можливість надати доступ в режимі редагування або тільки для читання, або заборонити доступ до CLI;

Можливість інтеграції з контролером Cisco ACI, що дозволяє вставляти міжмережевий екран NGFW між EPG як послугу рівня 4 до рівня 7, що дозволяє інспектувати трафік схід-захід (East-West) між рівнями програм у цих EPG та трафік північ-південь (North-South) між користувачами та програмами.

Можливість конвертації Snort та Suricata сигнатур для IPS-підсистем керованих NGFW.

### 4.4.10. Вимоги до сервісної підтримки NGFW

Сервісна підтримка програмного забезпечення не менше ніж 36 місяців , в тому числі з можливістю:

- Локального звернення до першої лінії підтримки від виробника NGFW в Україні із сертифікованими інженерами;
- Звернення телефоном або через Інтернет (чат та електронна пошта);
- Доступу до завантаження оновлень, виправлень;
- Доступу до документації.

## 4.5. IV. Програмна продукція - Підсистема для забезпечення захисту веб-додатків – 1 комплект

### 4.5.1. Загальні вимоги Покупця до програмної продукції

Підсистема призначена для забезпечення захисту веб-додатків шляхом перевірки, виявлення та блокування згідно налаштованих правил захисту додатків від шкідливого трафіка, метою якого є вивід з ладу серверів веб-додатків, отримання несанкціонованого доступу до даних веб-додатків та веб-сервісів.

### 4.5.2. Ліцензування

Підсистема має бути ліцензована для роботи протягом 36 місяців.

### 4.5.3. Загальні вимоги до запропонованого рішення

Наявність апаратних і віртуальних пристроїв з однаковою функціональністю;

Підтримка однакових налаштувань шифрування SSL / TLS на фізичних і віртуальних пристроях виробника рішення.

Можливість мігрувати конфігурацію від апаратного пристрою до віртуального такого ж виробника без втрати функціональності і без переривання обслуговування.

Підтримка платформ віртуалізації ESXi, KVM, Hyper-V, AWS, MS Azure.

Всі наступні функції повинні бути реалізовані в рамках одного віртуального/апаратного пристрою.

### 4.5.4. Вимоги до віртуального пристрою

4.5.4.1. Показники продуктивності:

• Пропускна здатність L4 рівня 200Mbps з можливістю ліцензованого розширення до 10 Gbit/s;

• Пропускна здатність L7 рівня 200Mbps з можливістю ліцензованого розширення до 10 Gbit/s;

• Кількість TCP з'єднань на секунду - 2 000 з можливістю збільшення до 135 000.

• Максимальна кількість одночасних TCP-сесій - 1 000 000 з можливістю збільшення до 10 000 000.

• Кількість запитів L7 рівня в секунду - 3 000 з можливістю збільшення до 450 000

• Продуктивність стиснення трафіку - 200Mbps

• Продуктивність SSL-шифрування трафіку - 200Mbps

• Продуктивність SSL TPS (2k keys) - 900 TPS з можливістю збільшення до 3 800 TPS (RSA); 1200 TPS з можливістю збільшення до 20 000 TPS (ECC).

4.5.4.2. Відмовостійкість і масштабування:

Схеми відмовостійкості і кластеризації:

• Повинна підтримуватися схема Load Sharing (Active / Active), схема Standby (Active / Passive).

• Максимальна кількість пристроїв у схемі Load Sharing/Standby – 8.

• Повинна забезпечуватися можливість об'єднання як фізичних, так і віртуальних пристроїв у відмовостійку схему.

• Повинна забезпечуватися можливість об'єднання різних моделей пристроїв в єдину відмовостійку схему.

• Повинна забезпечуватися підтримка можливості передачі обробки SSL- трафіку на пристрої з апаратним прискорювачем у рамках відмовостійкої схеми.

• Повинне забезпечуватися збереження стану сесій у момент перемикання між пристроями у відмовостійкій схемі.

• Повинен забезпечуватися механізм Graceful Shutdown для оброблюваних сесій у відмовостійкій схемі роботи.

• Можливість завантажити останню робочу конфігурацію з логічного розділу на диску без необхідності відновлення з резервної копії.

### 4.5.5. Вимоги до мережевої взаємодії

4.5.5.1. Взаємодія на L2 рівні

• Підтримка 802.1q VLAN, VLAN Groups.

• Підтримка STP.

• Підтримка LACP.

• Підтримка LLDP.

• Підтримка VXLAN, NVGRE.

• Підтримка L2TP, PPTP, PPP.

4.5.5.2. Взаємодія на L3 рівні

• Підтримка IPv4 та IPv6, IPX/SPX.

• Підтримка NAT, PAT, SNAT.

• Підтримка lan-to-lan IPSec, GRE-тунелювання.

• Підтримка QoS.

• Підтримка WCCP.

• Підтримка функції фільтрації пакетів.

• Підтримка статичної маршрутизації.

• Опціональна підтримка протоколів маршрутизації BGP, OSPF, EIGRP, IS - IS, RIP, Static.

• Підтримка VRF.

• Підтримка VRRP.

• Для інтерфейсу керування має бути ізольована таблиця маршрутизації.

### 4.5.6. Вимоги до системних функцій рішення

4.5.6.1.Керування модулями рішення

• Повинна забезпечуватися можливість додавання/видалення функціональних модулів рішення.

• Додавання/видалення функціональних модулів повинне відбуватися без зміни конфігурації апаратних засобів.

• Додавання/видалення функціональних модулів повинно відбуватися без необхідності інсталяції додаткового програмного забезпечення.

• Повинно забезпечуватися гарантоване виділення ресурсів під кожен функціональний модуль.

• Повинен забезпечуватися контроль використання ресурсів при додаванні/видаленні функціональних модулів.

4.5.6.2.Керування SSL - сертифікатами

• Повинна забезпечуватися можливість шифрування/дешифрування SSL- трафіку.

• Повинна забезпечуватися можливість додавання/видалення сертифікатів для SSL-трафіку.

• Повинна забезпечуватися можливість моніторингу стану сертифікатів SSL- трафіку.

4.5.6.3.Рольова модель розмежування прав користувачів системи

Каталог користувачів:

• Повинна підтримуватися інтеграція з LDAP.

• Повинна підтримуватися інтеграція з RADIUS.

• Повинна підтримуватися інтеграція з TACACS.

• Повинна підтримуватися інтеграція з Microsoft AD.

• Повинна підтримуватися інтеграція з ClientCert LDAP.

• Повинен забезпечуватися локальний каталог користувачів.

Повинен забезпечуватися механізм розподілу ролей користувачів для доступу до рішення.

Повинен забезпечуватися механізм розділення конфігурації на логічному рівні з наданням до неї прав доступу.

Повинно забезпечуватися розділення пристрою на декілька адміністративних розділів для доступу різними групами користувачів без обмеження функціонала налаштування.

4.5.6.4.Керування системними журналами

Повинна забезпечуватися можливість вивантаження системних журналів в режимі реального часу на стороннє програмне забезпечення.

Повинен забезпечуватися функціонал управління правилами фільтрації системних журналів.

Повинен забезпечуватися механізм розмежування прав доступу користувачів до системних журналів.

Повинен забезпечуватися функціонал управління конфігурацією рівня повідомлень системного журналу як з GUI- інтерфейсу, так і з CLI- інтерфейсу.

Повинен забезпечуватися функціонал управління системними журналами для кожного окремого модуля.

4.5.6.5. Керування резервними копіями конфігурації системи

Повинна забезпечуватися функція створення архіву усієї конфігурації рішення як з GUI-консолі, так і з CLI- консолі.

Повинна підтримуватися можливість створення різних версій архіву конфігурації.

Повинна підтримуватися можливість управління архівами конфігурації (створення, видалення, експорт, імпорт).

4.5.6.6.Моніторинг системи

Повинна забезпечуватися звітність продуктивності системи з такими параметрами:

• Об'єм оперативної пам'яті, що використовується.

• Продуктивність процесора.

• Утилізація кеш-пам'яті.

• Кількість активних сеансів, нових сеансів.

• Використовувана пропускна спроможність у біт/с, пакетів/с.

• Кількість HTTP запитів.

• Кількість SSL транзакцій.

Повинна забезпечуватися можливість моніторингу рішення стороннім програмним забезпеченням.

Повинна забезпечуватися підтримка наступних протоколів моніторингу:

• SNMP V1/2/3, SNMP Traps.

• sFlow/Netflow.

### 4.5.7. Вимоги до обробки SSL трафіку

4.5.7.1.Повинен забезпечуватися механізм SSL Offload, який дозволить перенести процес шифрування/дешифрування трафіку на апаратне рішення.

4.5.7.2.Повинен забезпечуватися механізм перенесення процесу шифрування або дешифрування SSL трафіку до/від користувача з серверів на пропоноване рішення.

4.5.7.3.Повинна забезпечуватися підтримка можливості передачі обробки SSL-трафіку на пристрої з апаратним прискорювачем у рамках відмовостійкої схеми.

4.5.7.4.Повинна забезпечуватися можливість відправки розшифрованого трафіку по ICAP на засоби його аналізу.

4.5.7.5.Повинні забезпечуватися індивідуальні правила роботи з SSL/TLS трафіком та його передачі на засоби аналізу на основі FQDN і/або IP адреси.

4.5.7.6.Повинна забезпечуватися можливість використання сторонніх центрів сертифікатів (Microsoft PKI).

4.5.7.7.Підсистема захисту від цільових атак і атак нульового дня мають бути інтегровані з підсистемою інспекції SSL.

### 4.5.8. Вимоги до системи балансування навантаження

4.5.8.1.Повинні забезпечуватися такі режими балансування навантаження:

- Стандартний режим балансування навантаження, що дозволяє термінувати сесії користувачів окремо від сесій серверів.

- Режим пересилки запитів L2 рівня.
- Режим пересилки запитів L3 рівня.
- Режим пересилки і апаратної акселерації запитів L4 рівня.
- Режим пересилки і апаратної акселерації HTTP запитів.
- Режим балансування пакетних протоколів.

4.5.8.2. Методи балансування

- Повинен забезпечуватися механізм балансування Round Robin.
- Повинен забезпечуватися механізм балансування Round Robin з використанням пріоритетів.
- Повинен забезпечуватися механізм балансування динамічного Round Robin.
- Повинен забезпечуватися механізм балансування з урахуванням кількості сесій на об'єкт у рамках ресурсу і у рамках сервера.
- Повинен забезпечуватися механізм балансування з урахуванням кількості сесій і використанням пріоритетів у рамках ресурсів і у рамках сервера.
- Повинен забезпечуватися механізм балансування з урахуванням швидкості роботи сервера.
- Повинен забезпечуватися самонавчальний механізм балансування.
- Повинна забезпечуватися можливість підключення резервних серверів для балансування.
- Повинен підтримуватися механізм створення спеціалізованих алгоритмів.

4.5.8.3.Моніторинг об'єктів балансування

4.5.8.3.1. Для контролю стану об'єктів балансування необхідно мати такі методи:

- Моніторинг з використанням DNS
- Моніторинг з використанням ICMP.
- Моніторинг з використанням ICMP- Gateway.
- Моніторинг з використанням TCP Echo.

4.5.8.3.2. Повинні забезпечуватися наступні методи моніторингу стану ресурсів:

- Моніторинг з використанням протоколу TCP.
- Моніторинг з використанням HTTP.
- Моніторинг з використанням HTTPS.
- Моніторинг з використанням HTTP та URL-адреси ресурсу.
- Моніторинг з використанням FTP.
- Моніторинг з використанням IMAP.
- Моніторинг з використанням LDAP.
- Моніторинг з використанням MSSQL.
- Моніторинг з використанням MySQL.
- Моніторинг з використанням RADIUS.
- Моніторинг з використанням SMTP.
- Моніторинг з використанням SOAP.
- Моніторинг з використанням UDP.
- Моніторинг з використанням WMI.
- Моніторинг з допомогою MQTT.
- Моніторинг з використанням NNTP.
- Моніторинг з використанням Oracle.
- Моніторинг з використанням SIP.
- Моніторинг з використанням SMB.

4.5.8.4.Має бути функція для створення спеціалізованих методів моніторингу ресурсів.

4.5.8.4.1. Повинен забезпечуватися механізм Graceful Shutdown для активних сесій користувачів у момент виведення об'єкту з процесу балансування.

4.5.8.4.2. Прив'язка сеансів до об'єкта балансування

- Повинен забезпечуватися функціонал прив'язки сеансів до об'єкту з використанням IP адрес джерела і одержувача.
- Повинен забезпечуватися функціонал прив'язки сеансів до об'єкту з використанням ідентифікатора сеансу.
- Повинен забезпечуватися функціонал прив'язки сеансів до об'єкту з використанням ідентифікатора сесії SSL.
- Повинен забезпечуватися функціонал прив'язки сеансів до об'єкту з використанням механізму Cookie.
- Повинен забезпечуватися функціонал прив'язки сеансів до об'єкту для MSRDP сеансів.
- Повинен забезпечуватися функціонал створення власних алгоритмів прив'язки користувача до об'єкту балансування.

4.5.8.4.3. Оптимізація трафіку

- Повинен забезпечуватися механізм компресії HTTP- трафіку.
- Повинен забезпечуватися механізм агрегації запитів різних користувачів в одну сесію до об'єкту балансування.
- Повинен забезпечуватися механізм SPDY.
- Повинен забезпечуватися механізм кешування часто використовуваного контенту.
- Наявність шаблонів попередньо налаштованих tcp, http-профілів, налаштування яких є кращою практикою для різних сценаріїв використання рішення, наприклад, wan мережі, lan мережі, мобільної мережі.

4.5.8.4.4. Програмування

- Повинен забезпечуватися механізм створення і керування спеціалізованими правилами і сценаріями обробки трафіку за допомогою засобів пропонованого рішення.
- Повинен забезпечуватися механізм створення і керування спеціалізованими правилами і сценаріями балансування навантаження за допомогою засобів пропонованого рішення.
- Повинен забезпечуватися механізм створення і керування спеціалізованих прив'язок сеансів до об'єктів засобами інтерфейсу пропонованого рішення.
- Повинна забезпечуватися можливість керування попередньо встановленими або спеціалізованими наборами конфігурацій сценаріїв балансування для додатків.
- Повинна забезпечуватися можливість керування попередньо встановленими або спеціалізованими наборами маніпуляції трафіком і його вмістом.

### 4.5.9. Вимога для захисту веб-ресурсів

4.5.9.1. Захист від DoS/DDoS атак рівня WEB ресурсу

4.5.9.1.1. Рішення повинне забезпечити очищення трафіку, спрямоване на зниження навантаження на ресурс, що атакується, шляхом виявлення і блокування паразитного трафіку для WEB ресурсу.

4.5.9.1.2. Рішення повинне забезпечувати очищення трафіку (атаки, що базуються на використанні протоколів http і https).

4.5.9.1.3. Повинно забезпечити реалізацію комплексу механізмів виявлення паразитного трафіку, при цьому забезпечувати використання наступних механізмів фільтрації:

4.5.9.1.3.1. Можливість у подальшому розширення функціоналу додатковою ліцензією для фільтрації запитів на основі репутаційної бази IP адрес:

4.5.9.1.3.1.1. Має бути механізм для керування базою репутаційних IP адрес.

4.5.9.1.3.1.1.1. Має бути механізм для керування базою репутаційних IP адрес.

4.5.9.1.3.1.1.2. Має бути механізм для створення як "чорних", так і "білих" списків IP адрес.

4.5.9.1.3.1.1.3. Має бути механізм класифікації "чорних" списків IP адрес.

4.5.9.1.3.1.1.4. Має бути механізм для налаштування різних правил обробки трафіку для різних категорій "чорного" списку IP адрес

4.5.9.1.3.1.2. Має бути механізм для створення як "чорних", так і "білих" списків IP адрес.

4.5.9.1.3.1.3. Має бути механізм класифікації "чорних" списків IP адрес.

4.5.9.1.3.1.4. Має бути механізм для налаштування різних правил обробки трафіку для різних категорій "чорного" списку IP адрес.

4.5.9.1.3.2. DOS/DDoS захист веб ресурсів на рівні 7 моделі OSI (Open Systems Interconnection):

4.5.9.1.3.2.1. Можливість блокування за такими критеріями:

4.5.9.1.3.1.2.1. IP адреса джерела.

4.5.9.1.3.1.2.2. Ідентифікатор пристрою.

4.5.9.1.3.1.2.3. URL.

4.5.9.1.3.1.2.4. Автоматично створених сигнатур.

4.5.9.1.3.2.2. Можливість запису трафіку під час атаки DDoS.

4.5.9.1.3.2.3. Можливості блокування атак:

4.5.9.1.3.2.3.1. Обмеження.

4.5.9.1.3.2.3.2. Блокування.

4.5.9.1.3.2.3.3. Captcha.

4.5.9.1.3.3. Повинен забезпечуватися захист від BotNet мереж:

4.5.9.1.3.3.1. Забезпечуватися категорізаційна база BotNet мереж.

4.5.9.1.3.3.2. Забезпечуватися індивідуальні правила обробки для кожної категорії.

4.5.9.1.3.3.3. Забезпечуватися механізм автоматичного визначення BotNet на базі вбудовуваного Javascript або поведінкового аналізу.

4.5.9.1.3.3.4. Забезпечуватися механізм захисту від BotNet на базі CAPTCHA.

4.5.9.1.3.3.5. Сторінка заглушка для ботів, які пройшли CAPTCHA.

4.5.9.1.3.3.6. Автоматичне визначення ботів на основі їх поведінки.

4.5.9.1.3.4. Фільтрація за географією (місцезнаходження джерела трафіку), як з можливістю виключення певних регіонів, так і з можливістю отримання трафіку тільки з певного переліку регіонів.

4.5.9.1.4. Мати можливість моніторингу трафіку ресурсів, що захищаються, на предмет виявлення аномалій і мати систему сповіщення про виявлені аномалії.

### 4.5.10. Захист веб ресурсів

4.5.10.1. Можливість захисту декількох веб-ресурсів на основі SNI та/або FQDN за різними політиками захисту індивідуально для кожного ресурсу.

4.5.10.2. Повинні надаватися механізми "digitally sign cookies", "encrypt cookies", and "rewrite URLs".

4.5.10.3. Повинні надаватися механізми "track session IDs", "prevent cookie injection, cookie tampering" та захист від "session hijacking attacks".

4.5.10.4. Необхідно підтримувати наступні методи блокування трафіку:

4.5.10.4.1. Block the HTTP request.

4.5.10.4.2. Block the connection.

4.5.10.4.3. Block the IP address.

4.5.10.4.4. Block the application session.

4.5.10.4.5. Block the user.

4.5.10.4.6. Send a TCP connection reset (in monitor mode).

4.5.10.4.7. Block the connection (in inline mode).

4.5.10.5. Забезпечити безпеку і цілісність вмісту XML відповідно до їх схем (а також SOAP, WSDL, JSON, AJAX).

4.5.10.6. Наявність вбудованого візарду для настройки захисту API.

4.5.10.7. Захист REST API.

4.5.10.8. Вбудована політика GraphQL API

4.5.10.9. Можливість створення політики API захисту на основі OpenApi файлу.

4.5.10.10. Правила безпеки для WebSocket.

4.5.10.11. Повинен забезпечуватися захист від повного переліку категорій атак на веб ресурси, визначених в останніх звітах OWASP Top 10.

4.5.10.12. Повинен забезпечуватися захист від "Zero Day Web Worm" атак.

4.5.10.13. Повинна забезпечуватися можливість інтеграції із такими сканерами вразливостей як: WhiteHat, IBM, Cenzic, HP, Qualys.

4.5.10.14. Методи побудови політик безпеки веб ресурсів:

4.5.10.14.1. Забезпечуватися автоматичне створення правил безпеки на основі реального трафіку веб ресурсів.

4.5.10.14.2. Забезпечуватися автоматичне створення правил безпеки на основі звітів сканерів вразливостей

4.5.10.14.3. Забезпечуватися автоматичне створення правил безпеки на попередньо встановлених шаблонах.

4.5.10.14.4. Забезпечуватися тонке налаштування існуючих правил безпеки в ручному режимі.

4.5.10.14.5. Забезпечуватися створення спеціалізованих правил безпеки для спеціалізованих веб ресурсів як в автоматичному, так і ручному режимі.

4.5.10.14.6. Можливість застосування правил блокування в режимі навчання без блокування.

4.5.10.14.7. Можливість доповнення існуючих політик безпеки результатами аналізу сканерів вразливостей.

4.5.10.15. Можливість відправки webhook подій.

4.5.10.16. Експертна оцінка кожної події політики безпеки веб ресурсів:

4.5.10.16.1. Визначатися міра загрози на веб ресурс.

4.5.10.16.2. Надаватися детальний опис загрози.

4.5.10.16.3. Надаватися детальний опис отриманого збитку на веб ресурс, що захищається.

4.5.10.16.4. Перелік пропонованих рекомендацій для зміни політики безпеки веб ресурсу.

4.5.10.16.5. Система повинна надавати рекомендації по змінах політики безпеки.

4.5.10.17. Можливість ліцензійного розширення функцій до визначення шахрайських дій шкідливого ПО при роботі з веб ресурсами на стороні користувача або дій Man-In-The-Middle.

4.5.10.18. Можливість у подальшому розширення функціоналу додатковою ліцензією для захисту мобільних додатків за допомогою інтеграції з SDK WAF.

4.5.10.19. Автоматичне визначення використовуваних технологій (ОС, веб сервер, технології веб ресурсу) на веб серверів.

4.5.10.20. Можливість у подальшому розширення функціоналу додатковою ліцензією для шифрування значень полів даних веб ресурсу на стороні користувача.

4.5.10.21. Інтеграція з антивірусом по протоколу ICAP.

4.5.10.22. Визначення автоматичного обходу CAPTCHA.

4.5.10.23. Визначення спроб обходу політики безпеки WAF.

4.5.10.24. Можливість створювати fingerprint клієнта з метою його відстежування, навіть в тих випадках, коли один користувач намагається використати декілька сесій.

4.5.10.25. Можливість у подальшому розширення функціоналу додатковою ліцензією для блокування на основі бази заражених fingerprint клієнтів.

4.5.10.26. Можливість у подальшому розширення функціоналу додатковою ліцензією для спроб входу за допомогою бази цих вкрадених паролів.

4.5.10.27. Підтримка і використання предвстановлених політик і звітів у тому числі для аудиту PCI DSS.

4.5.10.28. Можливість змінювати або додавати сигнатури.

4.5.10.29. Додаткові сигнатури від SoC виробника на основі поточних атак.

4.5.10.30. Повинна підтримувати створення власних типів вразливостей, правил їх визначення, їх опису і відображення як у внутрішній так і в системі моніторингу подій безпеки.

4.5.10.31. Можливість моніторингу працездатності веб ресурсу під захистом і перемикання трафіку на інший веб сервер у разі несправності основного веб ресурсу.

4.5.10.32. Можливість застосування необхідних виключень до політики безпеки по заблокованому або підозрілому запиту.

4.5.10.33. Захист HTTPS трафіку повинен забезпечуватися усіма правилами захисту веб ресурсу, присутніми в рішенні.

4.5.10.34. Можливість відбивати атаки Bruteforce на основі імені користувача, ідентифікатора пристрою, вихідного IP.

4.5.10.35. Здатність відбивати розподілені атаки Bruteforce.

4.5.10.36. Можливість роботи в пасивному режимі з дзеркалом трафіку, при цьому весь функціонал навчання журналювання і виявлення атак повинен працювати так само, як і в активному режимі, за винятком можливості блокування.

4.5.10.37. Система навчання повинна проходити навчання як на основі запитів, так і відповідей.

4.5.10.38. Побудова політики на основі результатів навчання повинна здійснюватися в автоматичному режимі – змінювати політику в режимі реального часу по готовності дослідження або за графіком і також у ручному режимі

4.5.10.39. Ієрархічне спадкування політик безпеки має підтримуватися.

4.5.10.40. Будь-які зміни в батьківській політиці повинні передаватися у спадок у правилах щодо дітей з можливістю налаштування успадкування тільки обраних елементів.

### 4.5.11. Вимоги до системи для надання та керування віддаленим доступом адміністраторів Підсистеми

4.5.11.1. Інтеграція з сервісами AAA (Authentication, Authorization and Accounting)

4.5.11.1.1. Повинна забезпечуватися інтеграція з Microsoft AD.

4.5.11.1.2. Повинна забезпечуватися інтеграція по LDAP.

4.5.11.1.3. Повинна забезпечуватися інтеграція з PKI для аутентифікації з використанням сертифікату.

4.5.11.1.4. Підтримка CRLDP.

4.5.11.1.5. Повинна забезпечуватися інтеграція з RADIUS.

4.5.11.1.6. Повинна забезпечуватися інтеграція з TACACS.

4.5.11.1.7. Повинна забезпечуватися інтеграція з RSA SecurID.

4.5.11.1.8. Повинна забезпечуватися інтеграція з IF - MAP server.

4.5.11.1.9. Повинна забезпечуватися інтеграція з HSM системами.

4.5.11.1.10. Повинна забезпечуватися інтеграція з Oracle Access Manager.

4.5.11.1.11. Повинна забезпечуватися інтеграція з OAuth.

4.5.11.1.12. Повинна забезпечуватися інтеграція з SAML 2.0

4.5.11.1.13. Підтримка багатофакторної аутентифікації.

4.5.11.1.14. Можливість генерації і верифікації OTP (one time password)

4.5.11.2. Правила керування доступом

4.5.11.2.1. Повинна забезпечуватися можливість створення політик доступу на основі облікового запису користувача.

4.5.11.2.2. Повинна забезпечуватися можливість створення політик доступу на основі груп користувачів.

4.5.11.2.3. Повинна забезпечуватися можливість створення різних сценаріїв доступу користувача у рамках однієї політики.

4.5.11.2.4. Повинен забезпечуватися функціонал створення і керування динамічної web- сторінки для користувача.

4.5.11.2.5. Наявність web-сторінок, що конфігуруються, для аутентифікації користувачів.

4.5.11.2.6. Наявність інтерактивного модуля для покрокового налаштування правил доступу користувачів.

4.5.11.2.7. Можливість побудови політик для кожної сесії або кожного запиту;

4.5.11.2.8. Можливість ідентифікації користувача за допомогою логіна/пароля. Має бути передбачене введення з віртуальної клавіатури.

4.5.11.2.9. Можливість керувати правилами доступу користувачів відповідно до цих критеріїв:

• ОС користувача.
• Тип пристрою користувача.
• Дата час на пристрої користувача.
• IP геолокація.
• Зламаний пристрій (Jailbreak or Root).
• Підконтрольний або непідконтрольний пристрій.
• Перевірка наявності антивіруса і актуальності його версії та версії його антивірусної бази.
• Перевірка firewall.
• Перевірка шифрування жорсткого диска.
• Перевірка наявності файлу на платформах Mac, Linux і Windows.
• Перевірка запущеного процесу в ОС Apple, Linux.
• Перевірка сертифікату ПК.
• Перевірка версії ОС.
• Перевірка shared folder в ОС користувача.
• Перевірка стану агента в ОС.
• Перевірка параметрів в реєстрі Windows.

4.5.11.3. Керування доступом адміністраторів

4.5.11.3.1. Повинен забезпечуватися механізм доступу користувачів до ресурсів за допомогою SSL VPN.

4.5.11.3.2. Повинен забезпечуватися механізм "Always connected".

4.5.11.3.3. Повинен забезпечуватися механізм перевірки мобільних пристроїв на відповідність внутрішнім стандартам Покупця.

4.5.11.3.4. Наявність тонкого програмного клієнта.

4.5.11.3.5. Повинна забезпечуватися підтримка мобільних пристроїв на базі iOS, Windows і Android.

4.5.11.3.6. Повинен забезпечуватися механізм доступу користувачів до web-ресурсів.

4.5.11.3.7. Повинен забезпечуватися доступу користувачів за допомогою механізму тунелювання трафіку до конкретного ресурсу.

4.5.11.3.8. Повинен забезпечуватися механізм зміни Java аплетів, т.з. "Java patching".

4.5.11.3.9. Можливість виведення користувачеві:

- Вікна вибору з декількох опцій.
- Виведення повідомлення.
- Відправка індивідуального логу повідомлення.

4.5.11.3.10. Повинна забезпечуватися можливість призначити користувачеві:

- Призначення ACL.
- Призначення набору ресурсів.
- Призначення пулу.
- Призначення VFR і правил SNAT.
- Призначення правил SSO.
- Індивідуальний скрипт обробки трафіку.

### 4.5.12. Вимоги до системи захисту інфраструктури та додатків

4.5.12.1. Stateful Inspection Firewall

4.5.12.1.1. Керування правилами фільтрації трафіку:

4.5.12.1.1.1. Правила повинні управлятися як глобальним правилом (для всього трафіку), так і на рівні правил, що стосуються конкретних додатків.

4.5.12.1.1.2. Перенаправлення трафіку повинно здійснюватися тільки за певним переліком дозволених протоколів.

4.5.12.1.1.3. Повинна забезпечуватись можливість застосування дати закінчення терміну дії правила.

4.5.12.1.1.4. Повинна забезпечуватись можливість застосування розкладу терміну дії правила.

4.5.12.1.2. Наявність функція репутаційної бази даних IP-адрес :

4.5.12.1.2.1. Має забезпечуватись механізм управління репутаційною базою даних IP адрес.

4.5.12.1.2.2. Має забезпечуватися механізм створення як «чорних», так і «білих» списків IP адрес.

4.5.12.1.2.3. Має забезпечуватися механізм категоризації «чорних» списків IP адрес.

4.5.12.1.2.4. Повинен забезпечуватись механізм конфігурування різних правил обробки трафіку для різних категорій «чорного» списку IP-адрес.

4.5.12.1.3. Моніторинг спрацьовування правил фільтрації трафіку:

4.5.12.1.3.1. Повинен забезпечуватись механізм підрахунку кількості спрацювань правил.

4.5.12.1.3.2. Повинен забезпечуватися налаштований механізм журналювання спрацьовувань, що включає наступні параметри: Policy Name, Rule Name, Action, Date and Time, Destination FQDN, Destination Geolocation, Destination IP,

Destination Port, Drop Reason, Protocol, Source FQDN, Source User, Source Geolocation , Source IP, Source Port, NAT Information, VLAN.

4.5.12.1.3.3. Повинен забезпечуватися налаштований механізм журналювання спрацьовувань, що включає наступні події: Rule Match Accept/Drop/Reject, IP Errors, TCP Errors, TCP Events, Translations.

4.5.12.1.4. Наявність перевірки HTTP, SIP, DNS

4.5.12.1.5. SSH-проксі

4.5.12.2. Захист від DoS/DDoS атак мережевого рівня

4.5.12.2.1. Повинен забезпечити очищення трафіку, спрямоване на зниження навантаження на атакований ресурс шляхом виявлення і блокування паразитичного трафіку.

4.5.12.2.2. Повинен забезпечити очищення трафіку (атаки, засновані на використанні протоколів UDP і ICMP).

4.5.12.2.3. Повинна забезпечуватись реалізація набору механізмів виявлення паразитичного трафіку, забезпечуючи при цьому використання наступних фільтруючих механізмів.

### 4.5.13. Вимоги до підтримки

Виробник забезпечує підтримку на протязі 36 місяців в режимі 24/7.

## 4.6. Вимоги до складу та змісту робіт

Постачальник має надати наступні послуги з метою встановлення, налаштування та інтеграції комплектів програмної продукції для забезпечення функціонування галузевого центру кіберзахисту сфери охорони здоров'я (далі - ГЦК), яке описане вище:

1. Постачання програмної продукції для забезпечення функціонування ГЦК;
2. Встановлення, налаштування, та інтеграцію поставлених в рамках Договору комплектів відповідно до Технічних Вимог провести в такій послідовності:
   - Налаштування операційних систем та/або систем керування віртуалізацією (гіпервізори);
   - Розгортання підсистеми SIEM (Security information and event management) + SOAR (Security Orchestration, and Automated Response) для управління подіями інформаційної безпеки так як базової системи для збору подій;
   - Розгортання підсистеми NGFW (Next-Generation Firewall) для захисту мережі;
   - Розгортання підистеми PAM (Privileged Access Management) для делегування доступів до інформаційних систем;
   - Розгортання підсистеми WAF (Web Application Firewall) для захисту веб-додатків та вебресурсів;
   - Розгортання систем управління базами даних ГЦК;
   - Об'єднання всіх компонентів в єдиний програмний комплекс ГЦК;
   - Розгортання у разі потреби додаткового програмного забезпечення (включаючи бази даних, тощо), зазначеного Постачальником;
3. Розробка технічної документації.
4. Розробка порядок приймання комплексу та проведення приймальних випробуваннь.
5. Навчання персоналу Покупця.

### 4.7. Вимоги до встановлення, налаштування, та інтеграції

Перед виконанням встановлення, налаштування, та інтеграції Покупцем буде виконано наступні роботи та надано Постачальнику:

- необхідні налаштування з боку інформаційних систем, які необхідні для реалізації інтеграції з ними;
- надані канали зв'язку та усі необхідні дозволи для підключення інженерів Постачальника до інформаційної системи Покупця;
- підготовлені робочі місця аналітиків-операторів ГЦК;
- підготовлений перелік операторів-аналітиків та інших відповідальних осіб з боку Покупця;
- виділені усі необхідні апаратні ресурси для розгортання елементів комплексу ГЦК (згідно вимог вказаних у технічній документації)

Постачальник має виконати встановлення, налаштування, та інтеграцію поставлених в рамках Договору комплектів програмної продукції, а також провести приймальні випробування усіх функціональних систем ГЦК з тим, щоб було забезпечено їх функціонування в єдиному програмному комплексі у відповідності до вимог, зазначених у Технічних вимогах, включаючи:

- Операційні системи та/або системи керування віртуалізацією (гіпервізори);
- Програмне забезпечення системи WAF (Web Application Firewall);
- Програмне забезпечення системи PAM (Privileged Access Management);
- Програмне забезпечення кластеру NGFW (Next-Generation Firewall);
- Програмне забезпечення системи SIEM (Security information and event management) + SOAR (Security Orchestration, and Automated Response);
- Системи управління базами даних;
- Додаткове програмне забезпечення (включаючи бази даних, тощо), Постачальника.

### 4.8. Вимоги до документування

Постачальник має розробити та передати Покупцю наступну Технічну документаціюГЦК:

| № з/п | Найменування |
|---|---|
| 1 | Архітектура комплексу рішень ГЦК |
| 2 | Схеми мережевих зав’язків та інтеграції комплексу, опис інфраструктури |
| 3 | Технічне завдання для кожного із елементів комплексу |
| 4 | Керівництва операторів-аналітиків ГЦК |
| 5 | Програми та методики приймальних випробувань ГЦК |

### 4.9. Порядок приймання Системи

Постачальник має виконати приймальні випробування усіх поставлених, встановлених та налаштованих в рамках Договору комплектів програмної продукції з тим, щоб було забезпечено їх функціонування у відповідності до вимог, зазначених у Технічних вимогах.

4.9.1. Приймання ГЦК та його складових систем проводиться шляхом проведення приймальних випробувань. Приймальні випробування здійснюються приймальною комісією, в яку входять уповноважені представники Покупця, Постачальника та інші особи відповідно до вимог договору на виконання робіт;

4.9.2. Мета приймальних випробувань складається в підтвердженні працездатності компонентів підсистем і відповідності їх вимогам Технічних вимог;

4.9.3. Види, склад, обсяг і методи випробувань визначаються програмою приймальних випробувань. Програми приймальних випробувань розробляється Постачальником і узгоджується Покупцем не пізніше, ніж за 5 днів перед початком випробувань;

4.9.4. При виявленні під час приймальних випробувань недоліків, дефектів або інших відхилень від вимог технічного завдання, відповідні факти фіксуються в протоколі, в якому в тому числі вказується:
- перелік недоліків (дефектів);
- ступінь впливу зазначених недоліків на працездатність системи;
- необхідні терміни усунення недоліків (дефектів).

4.9.5. Протягом 10 робочих днів з моменту усунення недоліків, дефектів або інших відхилень від вимог до системи приймальна комісія повинна провести повторні приймальні випробування відповідної підсистеми (або у цілому) ГЦК.

4.9.6. Результати приймальних випробувань оформлюються протоколом, який підписується членами Приймальної комісії з боку Покупця. За фактом успішного проведення приймальних випробувань підписується Акт приймання Програмної продукції та Супровідних послуг.

### 4.10. Вимоги до навчання персоналу Покупця

Навчання персоналу Покупця з адміністрування модулів ГЦК повинно бути проведено перед приймальними випробуваннями, і полягає у наступному:

1. Постачальник проводить навчання не менше 3-х аналітиків-операторів ГЦК (за всіма підсистемами, які перераховані в Технічних вимогах);
2. Кількість навчань по кожній системі повинна бути на менше 2-х;
3. Кількість навчань по керуванню програмним комплексом не менше 3-х;
4. Формат навчання: вебінар.

Постачальник має розробити програму навчання та погодити її з Покупцем.
Постачальник має обгрунтувати оптимальний термін та методологію навчання.

## 5. Вимоги до гарантійного обслуговування

5.1. Післягарантійне технічне обслуговування або подовження гарантійного обслуговування Постачальником або виробником:

- По закінченні строку гарантійного обслуговування, за умовами аналогічними гарантійним та на підставі окремого договору.

5.2. З метою подальшого розвитку функціональності:

- Постачальник повинен забезпечити можливість оновлення для виправлення помилок системи від виробника безкоштовно протягом усього періоду підтримки виробником, згідно з ліцензійною угодою та угодою технічної підтримки за умови наявності активного контракту технічної підтримки від виробника.
- Постачальник повинен надавати оновлення версій від виробника згідно ліцензійних угод на програмне забезпечення за умови наявності активного контракту технічної підтримки від виробника.

## 6. ГРАФІК ВПРОВАДЖЕННЯ

| № | Склад і зміст робіт | Коресподну ючі пункти Технічних вимог | Термін виконання (в календарних днях*) |
|---|---|---|---|
| **1** | Постачання програмної продукції для забезпечення функціонування ГЦК | 4.2.- 4.5 | до 10 днів по кожній з програмній продукції зазначеній в п. 4.1. з дати отримання відповідної заявки на поставку від Покупця але не пізніше ніж 90 днів з дати укладення договору. |
| **2** | Послуги із встановлення, налаштування та інтеграції програмної продукції | 4.7 | до 120 днів з дати підписання договору |
| **3** | Розробка технічної документації | 4.8 | до 120 днів з дати підписання договору |
| **4** | Розробка порядку приймання комплексу та проведення приймальних випробуваннь. | 4.9 | до 130 днів з дати підписання договору |
| **5** | Навчання персоналу Покупця | 4.10 | до 150 днів з дати підписання договору |

## 7. КВАЛІФІКАЦІЙНІ ВИМОГИ

**7.1. Досвід виконання аналогічного (аналогічних) за предметом закупівлі договору (договорів)**

Постачальник повинен бути досвідченим та кваліфікованим з виконання аналогічних за предметом закупівлі договорів, а саме мати досвід успішного виконання щонайменше одного договору протягом останніх 5 (п’яти) років, а саме з 01.01.2018.

Для цілей цієї вимоги аналогічним вважається договір *предметом якого є постачання будь якої програмної продукції (далі – ПЗ), а саме примірників програмного забезпечення або договір в складі якого постачались примірники програмного забезпечення з чітким*

*зазначенням програмного забезпечення, що постачалось за договором, та послуги з інсталяції або налаштування цього програмного забезпечення*

## 8. Вимоги до оформлення технічної пропозиції

### 8.1. Опис Інформаційних технологій, Матеріалів, інших Товарів, Послуг

8.1.1. Учасник повинен надати докладний опис головних технічних, експлуатаційних чи інших відповідних характеристик усіх головних Інформаційних технологій, Матеріалів, інших Товарів та Послуг, пропонованих у ціновій пропозиції (напр., номери версії, редакції та моделі). Без надання достатніх, чітких подробиць Учасники постають перед ризиком оголошення їх цінової пропозиції такою, що не відповідає вимогам.

8.1.2. Для полегшення оцінювання пропозицій докладний опис повинен бути організований та містити перехресні посилання в такому ж порядку, як пояснення Учасника по пунктам у Технічних вимогах. В інформації перехресних посилань потрібно, як мінімум, зазначити точні заголовки та номери сторінок.

8.1.3. Учасник в пропозиції повинен надати вимоги до ключових показників сервісів ІТ-інфраструктури.

8.1.4. Учасник в складі пропозиції надає детальний регламент підтримки програмного забезпечення з обов'язковим врахуванням вимог п. 5 Вимоги до гарантійного обслуговування.

### 8.2. Пояснення до Технічних вимог по пунктам

8.2.1. Учасник повинен надати пояснення по пунктам до Технічних вимог Покупця, які доводять відповідність по суті проекту Системи в цілому та окремих Інформаційних технологій, Товарів та Послуг, пропонованих за цими Вимогами.

8.2.2. Всі Технічні вимоги є обов'язковими. Учасник торгів повинен підтвердити відповідніст кожній вимозі та надати перехресні посилання на відповідний розділ технічної пропозиції.

8.2.3. Для того, щоб довести відповідність своєї пропозиції, настійливо радимо Учаснику торгів скористатися Контрольним списком Технічної відповідності, наданому у пункті 9 Технічних вимог. Якщо цього не зробити, значно зростає ризик оголошення пропозиції Учасника такою, що не відповідає технічним вимогам. Крім усього іншого, контрольний список повинен містити чіткі перехресні посилання на відповідні сторінки Технічної пропозиції Учасника.

### 8.3. Попередній План Проекту

8.3.1. Учасник повинен підготувати Попередній План Проекту, та описати, крім усього іншого, методи, людські та матеріальні ресурси, які Учасник торгів пропонує залучити до роботи над проектом, управління, координації та виконання усіх своїх обов'язків, у разі, якщо він отримає Договір, а також – заплановану тривалість та строк завершення усіх основних робіт. Попередній проект має відповідати термінам визначеним в пункті 6. Графік впровадження та враховували склад і зміст робіт.

### 8.4. Підтвердження відповідальності за інтеграцію та взаємодію інформаційних технологій

8.4.1. Учасник повинен подати письмове підтвердження, що у разі отримання Договору він бере на себе відповідальність за успішну інтеграцію та взаємодію усіх пропонованих Інформаційних технологій, включених у Систему, як зазначається у Запиті цінових пропозицій.

## 9. Контрольний список технічної відповідності

**Пояснення для Учасників**: Контрольний список надається, щоб допомогти Учаснику організувати та відповідно оформити свою технічну частину своєї пропозиції. За кожною з наступних Технічних вимог Учасник торгів повинен викласти, яким чином його Технічна пропозиція відповідає кожній вимозі. Крім того, Учасник торгів повинен надати перехресні посилання на відповідну допоміжну інформацію, якщо є, у складі пропозиції. Перехресне посилання повинне вказати відповідний документ(и), номер сторінки (сторінок), та параграф(и). Контрольний список технічної відповідності не заміняє решту Технічних вимог (або будь-яку іншу частину Запиту цінових пропозицій). Якщо вимога не згадується у Контрольному списку, це не звільняє Учасника торгів від відповідальності за внесення допоміжного свідчення відповідності цій іншій вимозі Технічної пропозиції. Відповіді, що складаються з одного чи двох слів (напр., „Так", „Ні", „Буде відповідним") зазвичай не є достатніми для підтвердження технічної відповідності Технічним вимогам.

Всі вимоги є обов'язковими.

*Покупець далі наводить примірник контрольного списку, який є уніфікованою формою, яку повинні притримуватися всі учасники.*

| № | Вимога | Статус | Розділ |
|---|---|---|---|
| **В 1.** | **Програмна продукція - Підсистема управління подіями інформаційної безпеки (SIEM+SOAR) на 5000 EPS:** | | **4.2** |
| В 1.1 | Загальні вимоги Покупця до програмної продукції | | Розділ 4.2.1. |
| Технічне обґрунтування відповідності з боку Учасника:<br>*(Заповнюється Учасником)* | | | |
| Перехресні посилання Учасника на допоміжну інформацію у Технічній документації:<br>*(Заповнюється Учасником, надається інформація з посиланням на сторінку в технічній документації, яка додається)* | | | |
| В 1.2 | Архітектура підсистеми | | Розділ 4.2.2. |
| Технічне обґрунтування відповідності з боку Учасника: | | | |
| Перехресні посилання Учасника на допоміжну інформацію у Технічній документації: | | | |
| В 1.3 | **Ліцензування** | | Розділ 4.2.3. |
| Технічне обґрунтування відповідності з боку Учасника: | | | |
| Перехресні посилання Учасника на допоміжну інформацію у Технічній документації: | | | |
| В 1.4 | **Вимоги до підсистеми** | | Розділ 4.2.4. |
| Технічне обґрунтування відповідності з боку Учасника: | | | |
| Перехресні посилання Учасника на допоміжну інформацію у Технічній документації: | | | |
| В 1.5 | **Функціональність підсистеми** | | Розділ 4.2.5. |
| Технічне обґрунтування відповідності з боку Учасника: | | | |
| Перехресні посилання Учасника на допоміжну інформацію у Технічній документації: | | | |
| В 1.6 | **Збір подій** | | Розділ 4.2.6. |
| Технічне обґрунтування відповідності з боку Учасника: | | | |

| № | Вимога | Статус | Розділ |
|---|---|---|---|
| | | | |
| Перехресні посилання Учасника на допоміжну інформацію у Технічній документації: | | | |
| В 1.7 | **Нормалізація подій** | | Розділ 4.2.7. |
| Технічне обґрунтування відповідності з боку Учасника: | | | |
| Перехресні посилання Учасника на допоміжну інформацію у Технічній документації: | | | |
| В 1.8 | **Кешування** | | Розділ 4.2.8. |
| Технічне обґрунтування відповідності з боку Учасника: | | | |
| Перехресні посилання Учасника на допоміжну інформацію у Технічній документації: | | | |
| В 1.9 | **Модуль зберігання та звітності** | | Розділ 4.2.9. |
| Технічне обґрунтування відповідності з боку Учасника: | | | |
| Перехресні посилання Учасника на допоміжну інформацію у Технічній документації: | | | |
| В 1.10 | **Відмовостій-кість та резервування** | | Розділ 4.2.10. |
| Технічне обґрунтування відповідності з боку Учасника: | | | |
| Перехресні посилання Учасника на допоміжну інформацію у Технічній документації: | | | |
| В 1.11 | **Захищеність підсистеми** | | Розділ 4.2.11. |
| Технічне обґрунтування відповідності з боку Учасника: | | | |
| Перехресні посилання Учасника на допоміжну інформацію у Технічній документації: | | | |
| В 1.12 | **Управління подіями і даними** | | Розділ 4.2.12. |
| Технічне обґрунтування відповідності з боку Учасника: | | | |
| Перехресні посилання Учасника на допоміжну інформацію у Технічній документації: | | | |
| В 1.13 | **Обробники подій (parsers)** | | Розділ 4.2.13. |
| Технічне обґрунтування відповідності з боку Учасника: | | | |
| Перехресні посилання Учасника на допоміжну інформацію у Технічній документації: | | | |
| В 1.14 | **Агентське ПЗ (для Windows)** | | Розділ 4.2.14. |
| Технічне обґрунтування відповідності з боку Учасника: | | | |
| Перехресні посилання Учасника на допоміжну інформацію у Технічній документації: | | | |
| В 1.15 | **Візуалізація і аналітика** | | Розділ 4.2.15. |
| Технічне обґрунтування відповідності з боку Учасника: | | | |
| Перехресні посилання Учасника на допоміжну інформацію у Технічній документації: | | | |
| В 1.16 | **Управління інцидентами та вразливостями** | | Розділ 4.2.16. |

| № | Вимога | Статус | Розділ |
|---|---|---|---|
| Технічне обґрунтування відповідності з боку Учасника: | | | |
| Перехресні посилання Учасника на допоміжну інформацію у Технічній документації: | | | |
| В 1.17 | **Інтеграція з зовнішніми джерелами інформації щодо загроз (Threat Intelligence)** | | Розділ 4.2.17. |
| Технічне обґрунтування відповідності з боку Учасника: | | | |
| Перехресні посилання Учасника на допоміжну інформацію у Технічній документації: | | | |
| В 1.18 | **Інтеграція з зовнішніми системами, розширення даних щодо інцидентів** | | Розділ 4.2.18. |
| Технічне обґрунтування відповідності з боку Учасника: | | | |
| Перехресні посилання Учасника на допоміжну інформацію у Технічній документації: | | | |
| **В 2.** | **Програмна продукція - Підсистема аудиту дій користувачів та надання доступу до критично важливих систем:** | | **4.3** |
| В 2.1 | **Загальні (системні) вимоги** | | Розділ 4.3.1. |
| Технічне обґрунтування відповідності з боку Учасника: | | | |
| Перехресні посилання Учасника на допоміжну інформацію у Технічній документації: | | | |
| В 2.2. | **Ліцензування** | | Розділ 4.3.2. |
| Технічне обґрунтування відповідності з боку Учасника: | | | |
| Перехресні посилання Учасника на допоміжну інформацію у Технічній документації: | | | |
| В 2.3 | **Функціональні (технічні) вимоги** | | Розділ 4.3.3. |
| Технічне обґрунтування відповідності з боку Учасника: | | | |
| Перехресні посилання Учасника на допоміжну інформацію у Технічній документації: | | | |
| В 2.4 | **Вимоги до функціоналу контролю привілейованих користувачів** | | Розділ 4.3.4. |
| Технічне обґрунтування відповідності з боку Учасника: | | | |
| Перехресні посилання Учасника на допоміжну інформацію у Технічній документації: | | | |
| В 2.5 | **Вимоги до підтримки** | | Розділ 4.3.5. |
| Технічне обґрунтування відповідності з боку Учасника: | | | |
| Перехресні посилання Учасника на допоміжну інформацію у Технічній документації: | | | |
| **В 3.** | **Підсистема для фільтрації мережевого трафіку та захисту мережі, аналізу запобігання мережевих вторгнень:** | | **4.4** |
| В 3.1 | **Ліцензування** | | Розділ 4.4.1. |
| Технічне обґрунтування відповідності з боку Учасника: | | | |

| № | Вимога | Статус | Розділ |
|---|---|---|---|
| Перехресні посилання Учасника на допоміжну інформацію у Технічній документації: | | | |
| В 3.2 | **Вимоги до продуктивності** | | Розділ 4.4.2. |
| Технічне обґрунтування відповідності з боку Учасника: | | | |
| Перехресні посилання Учасника на допоміжну інформацію у Технічній документації: | | | |
| В 3.3 | **Вимоги до параметрів розгортання** | | Розділ 4.4.3. |
| Технічне обґрунтування відповідності з боку Учасника: | | | |
| Перехресні посилання Учасника на допоміжну інформацію у Технічній документації: | | | |
| В 3.4 | **Вимоги до підтримуваних протоколів і режимів функціонування** | | Розділ 4.4.4. |
| Технічне обґрунтування відповідності з боку Учасника: | | | |
| Перехресні посилання Учасника на допоміжну інформацію у Технічній документації: | | | |
| В 3.5 | **Вимоги до відмовостійкості** | | Розділ 4.4.5. |
| Технічне обґрунтування відповідності з боку Учасника: | | | |
| Перехресні посилання Учасника на допоміжну інформацію у Технічній документації: | | | |
| В 3.6 | **Вимоги до функціоналу Підсистеми** | | Розділ 4.4.6. |
| Технічне обґрунтування відповідності з боку Учасника: | | | |
| Перехресні посилання Учасника на допоміжну інформацію у Технічній документації: | | | |
| В 3.7 | **Вимоги до можливостей запобігання вторгнень, розпізнавання й блокування шкідливого або забороненого трафіка в Підсистемі** | | Розділ 4.4.7. |
| Технічне обґрунтування відповідності з боку Учасника: | | | |
| Перехресні посилання Учасника на допоміжну інформацію у Технічній документації: | | | |
| В 3.8 | **Додаткові обов’язкові вимоги до NGFW** | | Розділ 4.4.8. |
| Технічне обґрунтування відповідності з боку Учасника: | | | |
| Перехресні посилання Учасника на допоміжну інформацію у Технічній документації: | | | |
| В 3.9 | **Вимоги до системи керування Програмними комплексами мережевої безпеки** | | Розділ 4.4.9. |
| Технічне обґрунтування відповідності з боку Учасника: | | | |
| Перехресні посилання Учасника на допоміжну інформацію у Технічній документації: | | | |
| В 3.10 | **Вимоги до сервісної підтримки NGFW** | | Розділ 4.4.10. |
| Технічне обґрунтування відповідності з боку Учасника: | | | |
| Перехресні посилання Учасника на допоміжну інформацію у Технічній документації: | | | |

| № | Вимога | Статус | Розділ |
|---|---|---|---|
| | | | |
| **В 4.** | **Підсистема для забезпечення захисту веб-додатків:** | | **4.5** |
| В 4.1 | **Загальні вимоги Покупця до програмної продукції** | | Розділ 4.5.1. |
| Технічне обґрунтування відповідності з боку Учасника: | | | |
| Перехресні посилання Учасника на допоміжну інформацію у Технічній документації: | | | |
| В 4.2 | **Ліцензування** | | Розділ 4.5.2. |
| Технічне обґрунтування відповідності з боку Учасника: | | | |
| Перехресні посилання Учасника на допоміжну інформацію у Технічній документації: | | | |
| В 4.3 | **Загальні вимоги до запропонованого рішення** | | Розділ 4.5.3. |
| Технічне обґрунтування відповідності з боку Учасника: | | | |
| Перехресні посилання Учасника на допоміжну інформацію у Технічній документації: | | | |
| В 4.4 | **Вимоги до віртуального пристрою** | | Розділ 4.5.4. |
| Технічне обґрунтування відповідності з боку Учасника: | | | |
| Перехресні посилання Учасника на допоміжну інформацію у Технічній документації: | | | |
| В 4.5 | **Вимоги до мережевої взаємодії** | | Розділ 4.5.5. |
| Технічне обґрунтування відповідності з боку Учасника: | | | |
| Перехресні посилання Учасника на допоміжну інформацію у Технічній документації: | | | |
| В 4.6 | **Вимоги до системних функцій рішення** | | Розділ 4.5.6. |
| Технічне обґрунтування відповідності з боку Учасника: | | | |
| Перехресні посилання Учасника на допоміжну інформацію у Технічній документації: | | | |
| В 4.7 | **Вимоги до обробки SSL трафіку** | | Розділ 4.5.7. |
| Технічне обґрунтування відповідності з боку Учасника: | | | |
| Перехресні посилання Учасника на допоміжну інформацію у Технічній документації: | | | |
| В 4.8 | **Вимоги до системи балансування навантаження** | | Розділ 4.5.8. |
| Технічне обґрунтування відповідності з боку Учасника: | | | |
| Перехресні посилання Учасника на допоміжну інформацію у Технічній документації: | | | |
| В 4.9 | **Вимога для захисту веб-ресурсів** | | Розділ 4.5.9. |
| Технічне обґрунтування відповідності з боку Учасника: | | | |
| Перехресні посилання Учасника на допоміжну інформацію у Технічній документації: | | | |
| В 4.10 | **Захист веб ресурсів** | | Розділ 4.5.10. |
| Технічне обґрунтування відповідності з боку Учасника: | | | |

| № | Вимога | Статус | Розділ |
|---|---|---|---|
| | | | |
| Перехресні посилання Учасника на допоміжну інформацію у Технічній документації: | | | |
| В 4.11 | **Вимоги до системи для надання та керування віддаленим доступом адміністраторів Підсистеми** | | Розділ 4.5.11. |
| Технічне обґрунтування відповідності з боку Учасника: | | | |
| Перехресні посилання Учасника на допоміжну інформацію у Технічній документації: | | | |
| В 4.12 | **Вимоги до системи захисту інфраструктури та додатків** | | Розділ 4.5.12. |
| Технічне обґрунтування відповідності з боку Учасника: | | | |
| Перехресні посилання Учасника на допоміжну інформацію у Технічній документації: | | | |
| В 4.13 | **Вимоги до підтримки** | | Розділ 4.5.13. |
| Технічне обґрунтування відповідності з боку Учасника: | | | |
| Перехресні посилання Учасника на допоміжну інформацію у Технічній документації: | | | |

**[НАЗВА ПОСТАЧАЛЬНИКА]**
**Підпис уповноваженої особи:**
**Печатка компанії**
**Місце:**
**Дата:**

**[Примітка:** Будь ласка ПІДПИШІТЬ та поставте ПЕЧАТКУ на ВСІ сторінки цього документу.]

**ДОДАТОК 3**

до Запиту до подання цінових пропозицій № HEAL-RFQ-4.1.1.9.

**[НА БЛАНКУ ОРГАНІЗАЦІЇ]**

## ЦІНОВА ПРОПОЗИЦІЯ

Міністерство охорони здоров'я України

01601, Україна, Київ,
вул. М. Грушевського, 7

Шановні панове,

Ми пропонуємо виконання договору № HEAL-RFQ-4.1.1.9 «Забезпечення функціонування Галузевого центру кібербезпеки сфери охорони здоров'я» відповідно до «Умов надання послуг» та «Технічних вимог», які надаються разом із цією ціновою пропозицією, за ціною договору _____*(сума прописом і цифрами)* (_____) *(назва валюти)*.

Ця цінова пропозиція і ваше письмове повідомлення про її прийняття становитимуть зобов'язання укласти з вами договір за формою, наведеною у Запиті до подання цінових пропозицій № HEAL-RFQ-4.1.1.9. Ми розуміємо, що ви не зобов'язані приймати цінову пропозицію з найнижчою ціною, або будь-яку іншу цінову пропозицію, отриману вами.

Цим документом ми підтверджуємо, що:

а) дана цінова пропозиція є дійсною протягом шістидесяти (60) днів з кінцевої дати надання цінової пропозиції зазначеної у п.5 Запиту до подання цінових пропозицій № HEAL-RFQ-4.1.1.9.

б) Постачальник та / або запропоноване програмне забезпечення чи його компоненти не підпадають під обмежувальні заходи (санкції) введені відповідно до чинних Указів Президента України.

_____ Дата: _____

[Підпис уповноваженої особи Постачальника] [День/Місяць/Рік]

П.І.Б. уповноваженої особи Постачальника: _____

Назва Постачальника: _____
Адреса: _____
_____
Тел. _____
Факс _____

Додаток 1: Умови надання послуг
Додаток 2: Технічні вимоги
Додаток 3: Форма «Інформація про досвід та інституційну спроможність»

**[Примітка:** Будь ласка ПІДПИШІТЬ та поставте ПЕЧАТКУ на ВСІ сторінки цього документу.]

**ДОДАТОК 4**

до Запиту до подання цінових пропозицій № HEAL-RFQ-4.1.1.9.

## ІНФОРМАЦІЯ ПРО ДОСВІД ТА ІНСТУЦІЙНУ СПРОМОЖНІСТЬ

1. **Досвід виконання аналогічного (аналогічних) за предметом закупівлі договору (договорів)**

[Використовуючи форму, наведену нижче, просимо надати стислий опис, включаючи досвід (в роках) надання специфічних послуг що мають відношення до завдання.]

| | |
|---|---|
| **Повна назва Учасника** | |
| **Досвід надання аналогічних послуг** | |
| **Юридична адреса Учасника** | |
| Телефон:<br>Ел.пошта (веб-сторінка): | |

*[Використовуючи форму, наведену нижче, просимо надати інформацію про кожне завдання, що підтверджує наявність в Учасника відповідного досвіду]*

| Дата (період) | Назва завдання (договору)/стислий опис результатів | Назва Покупця | Приблизна вартість договору (еквівалент в доларах США) | Коротка технічна специфікація щодо стеку технологій, які застосовувались |
|---|---|---|---|---|
| | | *(найменування, адреса, контактні особи (прізвище та контактний телефон)* | | |
| | | | | |
| | | | | |
| | | | | |
| | | | | |

Для підтвердження виконання заявлених завдань необхідно надати:

- сканований договір/и, що зазначений/і у довідці (повинен передаватися у PDF-форматі, сканований з оригіналу документа, в кольоровому зображенні);

- акт наданих послуг по вищенаведеному договору з підписами та печатками обох сторін (за наявності печаток та у випадку їх використання в своїй господарській діяльності та при оформленні документів) або інші документи, що підтверджують факт повного виконання аналогічного договору.

При наданні вищезазначених документів Учасник може приховати відомості, які становлять комерційну таємницю, про що Учасник надає відповідну довідку.

** Під аналогічним договором, відповідно до умов цієї Документації, слід розуміти договір, предметом якого є постачання будь якопрограмної продукції (далі – ПЗ), а саме примірників програмного забезпечення або договір в складі якого постачались примірники програмного забезпечення з чітким зазначенням програмного забезпечення, що постачалось за договором, та послуги з інсталяції або налаштування цього програмного забезпечення*

**[НАЗВА ПОСТАЧАЛЬНИКА]**
**Підпис уповноваженої особи:**
**Печатка компанії**
**Місце:**
**Дата:**

**[Примітка:** Будь ласка ПІДПИШІТЬ та поставте ПЕЧАТКУ на ВСІ сторінки цього документу.]

[1] *Інформація, що подається Постачальником має бути максимальною повною та релевантною до встановлених вимог. Надання не повної, чи не достатньо деталізованої інформації а також підтверджуючих документів становить ризик Постачальника під час оцінки відповідності його досвіду і спроможностей встановленим кваліфікаційним вимогам*

**ДОДАТОК 5**

до Запиту до подання цінових
пропозицій № HEAL-RFQ-4.1.1.9.

**ДОГОВІР № HEAL-RFQ-4.1.1.9./___**

м. Київ _____ 2023 р.

Цей Договір укладено в день, місяць та рік, зазначені вище, між Міністерством охорони здоров'я України (далі – Покупець), в особі заступника Міністра охорони здоров'я України, _____, який діє на підставі наказу Міністерства охорони здоров'я України від _____ № _____, з однієї сторони, та _____ (далі - Постачальник) в особі _____, який діє на підставі Статуту, з іншої сторони, які надалі разом іменуються «Сторони», а кожен окремо «Сторона».

Договір укладається в рамках реалізації Проекту «Зміцнення системи охорони здоров'я та збереження життя в Україні» (HEAL Ukraine) (далі - Проект), що фінансується відповідно до Угоди про позику між Україною та Міжнародним банком реконструкції та розвитку (далі - Банк) від 22.12.2022 № 9468-UA (далі – Угода про позику).

## 1. ПРЕДМЕТ ДОГОВОРУ

1.1. Постачальник зобов'язується поставити Покупцеві програмну продукцію та надати супровідні послуги з її встановлення, налаштування, інтеграції а також навчання персоналу Покупця з метою забезпечення функціонування Галузевого центру кібербезпеки сфери охорони здоров'я (далі – Програмна продукція та супровідні Послуги), а Покупець зобов'язується придбати (прийняти та оплатити) Програмну продукцію та супровідні Послуги на умовах даного Договору.

1.2. Вартість, асортимент, кількість та технічні вимоги до Програмної продукції та супровідних Послуг вказуються в Додатку № 1 «Умови постачання» та Додатку № 2 «Технічні вимоги», які є невід'ємною частиною цього Договору.

1.3. Постачальник підписанням цього Договору визнає та підтверджує, що:

- на дату підписання цього Договору він має всі права та правові підстави, необхідні для виконання своїх зобов'язань за цим Договором, а також що Програмна продукція не порушує будь-який патент, авторські права та/або подібні права на інтелектуальну власність третіх осіб згідно з законодавством України. У разі якщо Постачальник на момент поставки Програмної продукції Покупцю ввів в оману останнього з приводу наявності у Постачальника таких прав, Постачальник зобов'язується відшкодувати Покупцю всі понесені Покупцем у зв'язку з цим збитки.

- укладення та виконання ним цього Договору не суперечить нормам законодавства України та відповідає його вимогам зокрема, щодо отримання та наявності усіх необхідних діючих дозволів та погоджень, а також підтверджує, що укладання та виконання ним цього Договору не суперечить цілям діяльності Постачальника, положенням його установчих документів, інших локальних актів тощо. Постачальник підписанням цього Договору підтверджує наявність всіх дозвільних документів на поставку Програмної продукції.

1.4. Якість Програмної продукції має відповідати характеристикам та вимогам її виробника, умовам цього Договору, додатків до цього Договору.

1.5. Право використання Програмної продукції поширюється на всю територію України.

1.6. Авторські та виключні майнові права на Програмну продукцію Покупцю не передаються.

1.7. Покупцю надається строкове і невиключне майнове право використання Програмної продукції за його функціональним призначенням, без права передачі/продажу/відчуження самої Програмної продукції та/або повноважень на його користування третім особам. Строк дії ліцензій (тобто строк права користування комп'ютерною програмою, права на одержання від Правовласника оновлень та підтримки комп'ютерної програми) – 36 місяців з дати підписання Акта приймання Програмної продукції, якщо інший строк не визначений в Додтаку 2 «Технічні вимоги».

1.8. В залежності від потреб Покупця, обсяги закупівлі можуть бути зменшені Покупцем в односторонньому порядку, шляхом направлення Покупцем Постачальнику відповідного повідомлення. При цьому, ціна Договору відповідним чином зменшується.

## 2. ПРАВА ТА ОБОВ'ЯЗКИ СТОРІН

**2.1. Постачальник зобов'язується:**

2.1.1. В порядку та на умовах, визначених у цьому Договорі, здійснити постачання Програмної продукції Покупцю та надання Супровідних послуг.

2.1.2. Надати Покупцю електронний ключ (код активації) або логін та пароль, що надають Покупцю можливість почати користуватися комп'ютерною програмою за умови приєднання Покупцем до ліцензійних умов Правовласника (факт приєднання Покупця до ліцензійних умов Правовласника підтверджує правомірність використання Покупцем Програмної продукції).

2.1.3. Нести всі ризики пов'язані з правомірністю використання Покупцем отриманих від Постачальника прав за цим Договором.

2.1.4. Надати Покупцю всі необхідні документи для прийому Програмної продукції.

2.1.5. Своєчасно вирішувати усі питання, пов'язані з якісним виконанням зобов'язань за цим Договором.

2.1.6. Усувати всі виявленні Покупцем у якості постачання Програмної продукції. Сторони розуміють, що:

2.1.6.1. Неякісне постачання – це неможливість Покупця почати користуватися Програмною продукцією за допомогою ключів активації, поставлених Постачальником Покупцю.

2.1.6.2. Постачальник не несе відповідальності за роботу Програмної продукції та не може впливати на роботу Програмної продукції, постачальник не відповідає за функціональні та інші можливості Програмної продукції.

2.1.7. Належним чином виконувати інші зобов'язання, пов'язані з виконанням цього Договору.

**2.2.Постачальник має право:**

2.2.1. Своєчасно та в повному обсязі отримувати оплату за поставлену Програмну продукцію та надані Супровідні послуги.

2.2.2. Достроково здійснити постачання Програмної продукції.

2.2.3. Ініціювати внесення змін до цього Договору.

2.2.4. Інші права передбачені цим Договором та законодавством України.

**2.3.Покупець зобов'язаний:**

2.3.1. Прийняти Програмну продукцію та належним чином надані Супровідні послуги у порядку та на умовах передбачених цим Договором.

2.3.2. Своєчасно та в повному обсязі сплатити за прийняту Програмну продукцію та надані Супровідні послуги.

2.3.3. Належним чином виконувати інші зобов'язання, пов'язані з виконанням Договору.

**2.4.Покупець має право:**

2.4.1. Контролювати постачання Програмної продукції та надання Супровідних послуг.

2.4.2. Вимагати належного виконання умов цього Договору.

2.4.3. Відмовитися від прийняття Програмної продукції та Супровідних послуг, які не відповідає вимогам та умовам цього Договору.

2.4.4. Вимагати від Правовласника підтримки Програмної продукції на умовах цього Договору, згідно Додатку 2 «Технічні вимоги».

2.4.5. Ініціювати внесення змін до цього Договору.

2.4.6. Інші права передбачені цим Договором та законодавством України.

## 3. СУМА ДОГОВОРУ та ОПЛАТА

3.1. Сума договору становить _____ включаючи усі податки, митні збори, доставку, завантаження, розвантаження та додаткові послуги включно із ПДВ у сумі _____. Сума Договору та одиничні ціни Товарів, вказані в Додатку № 1, є фіксованими і змінам не підлягають.

3.2. До ціни Договору включено усі витрати Постачальника, пов'язані з виконанням цього Договору, в тому числі сплата обов'язкових податків, зборів, а також інші витрати, які Постачальник здійснює на користь третіх осіб. Не врахована Постачальником вартість окремих витрат не сплачується Покупцем окремо та вважається зарахованою у ціні цього Договору.

3.3. Оплата за цим Договором здійснюється наступним чином:

***Варіант 1***

- Авансовий платіж: тридцять (30) відсотків загальної суми Договору сплачуються протягом тридцяти (30) календарних днів з дати підписання Договору за умови надання запиту та банківської гарантії на авансовий платіж на відповідну суму, що є дійсною до моменту доставки та прийому всіх Товарів та надається за формою, наведеною в Додатку № 4 або іншою формою, прийнятною для Покупця.
- Шістдесят (60) відсотків вартості відповідного комплекту програмної продукції буде сплачено Покупцем Постачальнику протягом тридцяти (30) календарних днів з дня надання Постачальником оригіналу рахунку-фактури та підписаного Сторонами Акту приймання Програмної продукції на відповідний поставлений комплект програмної продукції
- Десять (10) відсотків загальної вартості всіх комплектів програмної продукції та сімдесять (70) відсотків вартості Послуг із встановлення, налаштування, та інтеграції програмної продукції та вартості Навчання персоналу Покупця, протягом тридцяти (30) календарних днів з дня надання Постачальником оригіналу рахунку-фактури та підписаного Сторонами Акту надання Супровідних послуг після виконання Постачальником всіх зобов'язань за Договором, окрім гарантійних зобов'язань.

У разі відмінності валюти договору від української гривні – оплата буде здійснюватись в українській гривні за офіційним курсом Національного банку України на день підписання Покупцем видаткової накладної.

Банківська гарантія на авансовий платіж має бути видана авторитетною установою із правомочної країни за формою наведеною в Додатку 4.

Українська банківська установа, що видає заставне забезпечення, повинна мати довгостроковий кредитний рейтинг за національною шкалою не нижче «uaAA».

***Варіант 2***

- Дев'яносто (90) відсотків вартості відповідного комплекту програмної продукції буде сплачено Покупцем Постачальнику протягом тридцяти (30) календарних днів з дня надання Постачальником оригіналу рахунку-фактури та підписаного Сторонами Акту приймання Програмної продукції на відповідний поставлений комплект програмної продукції
- Десять (10) відсотків загальної вартості всіх комплектів програмної продукції та сто (100) відсотків вартості Послуг із встановлення, налаштування, та інтеграції програмної продукції та вартості Навчання персоналу Покупця, протягом тридцяти (30) календарних днів з дня надання Постачальником оригіналу рахунку-фактури та підписаного Сторонами Акту надання Супровідних послуг після виконання Постачальником всіх зобов'язань за Договором, окрім гарантійних зобов'язань.

У разі відмінності валюти договору від української гривні – оплата буде здійснюватись в українській гривні за офіційним курсом Національного банку України на день підписання Покупцем видаткової накладної.

3.4. Оплата за цим Договором здійснюється за рахунок коштів позики (Угода про позику між Україною та Міжнародним банком реконструкції та розвитку від 22 грудня 2022р. № 9468-UA), передбачених у спеціальному фонді державного бюджету.

3.5. На період дії воєнного стану в Україні оплата здійснюється у порядку черговості відповідно до Порядку виконання повноважень Державною казначейською службою в особливому режимі в умовах воєнного стану, затвердженого постановою Кабінету Міністрів України від 09 червня 2021 року № 590.

## 4. СТРОКИ ТА ПОРЯДОК ПРИЙМАННЯ-ПЕРЕДАЧІ ПРОГРАМНОЇ ПРОДУКЦІЇ ТА СУПРОВІДНИХ ПОСЛУГ

4.1. Поставка кожного із примірників Програмної продукції вказаних в додатку 1 «Умови постачання» здійснюється Постачальником у терміни вказані в п. 6 «Графік впровадження» Додтаку 2 «Технічні вимоги» і супроводжується отриманням Покупцем від Постачальника ключових файлів та/або цифрових кодів та/або ідентифікаторів Покупця, які забезпечують активацію поставленої Програмної продукції.

4.2. Поставка кожного із примірників Програмної продукції підтверджується підписанням повноважними представниками Сторін Акта приймання Програмної продукції, в якому відображається перелік Програмної продукції, на яку Покупець отримав право використання в межах цього Договору.

4.3. За результатами надання Послуг зі встановлення, налаштування та інтеграції програмної продукції та Навчання персоналу Покупця (обсяг завдання передбачений п. 4.7 – 4.10 Додатку 2 «Технічні Вимоги») Постачальник складає і підписує два примірники Акта надання Супровідних послуг та передає їх Покупцю.

4.4. Покупець протягом 5 (п'яти) робочих днів з дати отримання Акта(ів) приймання Програмної продукції або Акта надання Супровідних послуг підписує його або в той же строк надає Постачальнику письмову мотивовану відмову від його підписання.

4.5. У випадку отримання від Покупця відмови від підписання Акта(ів) приймання Програмної продукції або Акта надання Супровідних послуг, Постачальник зобов'язується в строк, визначений у відмові, усунути зауваження, після чого повторно надати відповідні Акти на підпис Покупцю.

4.6. Якщо після прийняття Програмної продукції чи Послуг із встановлення, налаштування та інтеграції програмної продукції Покупець виявив допущені Постачальником відступи від умов цього Договору або інші недоліки, які не могли бути виявлені під час звичайного способу прийняття (приховані недоліки), у тому числі приховані Постачальником, Покупець повідомляє про це Постачальника, а Постачальник зобов'язаний власними силами і за власний рахунок усунути виявлені недоліки протягом 10 (десяти) календарних днів з моменту отримання письмового повідомлення від Покупця. Прихованими недоліками за цим Договором визначаються такі недоліки, що виявлені після прийняття Покупцем Програмної продукції чи послуг із встановлення, налаштування та інтеграції програмної продукції в процесі використання, експлуатації тощо.

4.7. Усунення всіх зауважень здійснюється силами та за рахунок Постачальника.

## 5. ПРИПИНЕННЯ ДІЇ ДОГОВОРУ

5.1. Припинення дії у зв'язку з невиконанням договірних зобов'язань

(a) Покупець, без шкоди будь-яким іншим заходам, пов'язаним із порушенням умов Договору, може розірвати Договір цілком або частково, надіславши Постачальнику в письмовій формі повідомлення про невиконання останнім зобов'язань за Договором:

(i) у разі, якщо Постачальник неспроможний поставити всю Програмну продукцію чи її частину або надати Супровідні послуги в повному обсязі в межах періоду, визначеного в Договорі, або в межах будь-якого наданого його продовження;

(ii) у разі, якщо Постачальник неспроможний виконати будь-яке інше зобов'язання за Договором; або

(iii) у разі, якщо Постачальник, на думку Покупця, був замішаний у корупції або шахрайстві, як зазначено в п. 5 нижче в процесі конкуренції за отримання або виконання Договору.

(b) Якщо Покупець розриває Договір повністю або частково, Покупець може, на прийнятних умовах і в доцільний спосіб, закупити аналогічну непоставлену Програмну продукцію, причому Постачальник буде нести перед Покупцем відповідальність за всі додаткові витрати, пов'язані з такими аналогічною Програмною продукцією. Однак Постачальник повинен продовжувати виконання Договору в тій його частині, що не була розірвана.

5.2. Розірвання Договору в силу неплатоспроможності

(a) Покупець може в будь-який час розірвати Договір, направивши Постачальнику відповідне письмове повідомлення, якщо Постачальник стає банкрутом або в інший спосіб оголошується неплатоспроможним. В цьому випадку розірвання здійснюється без виплати компенсації Постачальнику за умови, що таке розірвання не шкодить або не впливає на будь-які права щодо дій або коригувальних заходів, що були чи будуть згодом набуті Покупцем.

5.3. Розірвання Договору в силу доцільності

(a) Покупець може в будь-який час повністю або частково розірвати Договір в силу доцільності, надіславши Постачальнику відповідне письмове повідомлення У цьому повідомленні повинно бути зазначено, що таке розірвання здійснюється з міркувань доцільності для Покупця, визначено обсяг анульованих зобов'язань Постачальника за Договором, а також дату вступу в силу такого розірвання.

## 6. ШАХРАЙСТВО ТА КОРУПЦІЯ

6.1. У разі, якщо Покупець виявить, що Постачальник та/або будь-хто з його працівників, агентів, субпідрядників, консультантів, надавачів послуг, постачальників та/або найманих працівників вдавались до корупційних або шахрайських дій, або до практики змови, примусу, перешкоджання розслідуванню в процесі конкурентного відбору або при виконанні цього Договору, у цьому випадку Покупець може припинити залучення Постачальника за Договором і дію Договору, письмово повідомивши про це Постачальника не пізніше, ніж за 14 днів до припинення дії Договору. При цьому положення пункту 5 застосовуються так ніби мало місце припинення дії Договору відповідно до пп.5.1.

6.2. Від Постачальника вимагається дотримання вимог Антикорупційного керівництва Банку та його переважаючих політик та процедур щодо санкцій, викладених в Санкційних правилах Банку, як визначено в Додатку 3 до Договору.

## 7. ПЕРЕВІРКИ ТА АУДИТ

7.1. Постачальник має виконувати всі вказівки Покупця, які відповідають чинному законодавству України.

7.2. Постачальник дозволяє Банку і/або особам, призначеним Банком, а також має забезпечити отримання дозволу від своїх Субпідрядників та консультантів, інспектувати і/або проводити на вимогу Банку аудит рахунків, записів та інших документів, що мають відношення до подання цінової пропозиції та виконання Договору. Звертаємо увагу Постачальника, його Субпідрядників та консультантів на п.6 Шахрайство та корупція, яким, окрім іншого, передбачається, що дії, спрямовані на суттєве обмеження реалізації Банком свого права на проведення перевірок та аудиту становить заборонену практику, яка тягне за собою розірвання договору і/або застосування Банком санкцій (включаючи визнання Постачальника неправомочним, але не обмежуючись цим) відповідно до стандартних процедур Банку щодо застосування санкцій.

## 8. ГАРАНТІЙНІ ЗОБОВ'ЯЗАННЯ

8.1. Постачальник гарантує якість Програмної продукції, яка поставляється за цим Договором.

8.2. Постачальник підтверджує гарантійні зобов'язання (далі – Гарантія) за цим Договором щодо Програмної продукції протягом гарантійного строку вказаного у цьому Договорі.

8.3. Гарантійний строк починає свій перебіг з дати підписання Акта приймання Програмної продукції та Супровідних послуг та діє впродовж періоду визначеного в Додатку 2 Технічні вимоги.

8.4. Гарантія надається у вигляді технічної підтримки Програмної продукції від Виробника Програмної продукції, яка включає в себе: надання оновлених версій Програмної продукції; доопрацювання Програмної продукції у випадку виявлення помилок, збоїв у роботі та/або виникнення позаштатних ситуацій; налаштування, супроводження діяльності Програмної продукції та надання консультацій щодо функціонування, використання Програмної продукції.

8.5. Технічна підтримка надається безпосередньо Виробником.

## 9. ОБСТАВИНИ НЕПЕРЕБОРНОЇ СИЛИ

9.1. Сторони звільняються від відповідальності за невиконання або неналежне виконання зобов'язань за цим Договором у разі виникнення обставин непереборної сили, які не існували

під час укладання цього Договору та виникли поза волею Сторін (аварія, катастрофа, стихійне лихо, епідемія, епізоотія, війна тощо).

9.2. Сторона, що не може виконувати зобов'язання за цим Договором внаслідок дії обставин непереборної сили, повинна не пізніше ніж протягом 5 (п'яти) днів з моменту їх виникнення повідомити про це іншу Сторону у письмовій формі.

9.3. Доказом виникнення обставин непереборної сили та строку їх дії є відповідні документи, які видаються уповноваженими на це законами України органами.

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

9.5. У разі здійснення Покупцем попередньої оплати та неможливості надання послуг Постачальником через настання обставин непереборної сили, Постачальник повертає Покупцю кошти протягом 3 (трьох) днів з дня розірвання Договору.

## 10. ВІДПОВІДАЛЬНІСТЬ СТОРІН

10.1. За невиконання або/та неналежне виконання умов даного Договору Сторони несуть майнову відповідальність згідно з даним Договором та діючим законодавством України.

10.2. За порушення строків поставки Програмної продукції та надання Супровідних послуг Покупець має право розірвати договір без будь-яких зобов'язань перед Постачальником в разі невиконання поставки Програмної продукції та ненадання Супровідних послуг через 21 день від крайнього терміну поставки Програмної продукції або надання Супровідних послуг, вказаному в Додатку 2 Технічні вимоги, після відповідного письмового повідомлення Покупцем.

10.3. За порушення строків поставки Програмної продукції або надання Супровідних послуг з Постачальника стягується неустойка у розмірі 0,2% від вартості відповідної Програмної продукції чи Супровідних послуг, щодо яких допущено прострочення, за кожен календарний день прострочення. Неустойка, що стягується, не має перевищувати 10% вартості недопоставленої у строк Програмної продукції чи не наданих Супровідних послуг.

10.4. Якщо Постачальник використовуватиме послуги субпідрядників, перевізників, експедиторів та інших компаній, які залучаються для своєчасного та належного виконання Договору, вся відповідальність перед Покупцем за будь-які втрати, збитки або за неналежне виконання Договору несе Постачальник.

## 11. ВИРІШЕННЯ СПОРІВ

11.1. Усі спори, що виникають внаслідок або у зв'язку з цим Договором, вирішуються шляхом переговорів між Сторонами.

11.2. Якщо Сторони не можуть дійти до згоди, то спір підлягає вирішенню у порядку, передбаченому чинним законодавством України.

## 12. СТРОК ДІЇ ДОГОВОРУ

12.1. Цей Договір набуває чинності в день підписання та діє до повного виконання Сторонами своїх зобов'язань, зокрема, в частині Постачання Програмної продукції та виконання Супровідних послуг – відповідно до термінів, визначених Додатку 2 Технічні вимоги, в частині розрахунків – до повного їх виконання, але не пізніше __ _____ 202_ року.

12.2. Договір складено в 2-х примірниках, які мають однакову юридичну силу, по одному для кожної Сторони.

## 13. ІНШІ УМОВИ

13.1. Усі зміни та доповнення до цього Договору здійснюються в письмовій формі шляхом укладення додаткових угод, що є невід'ємною частиною Договору.

13.2. Всі повідомлення будь-якої із Сторін цього Договору іншій Стороні повинні направлятись поштою, електронною поштою або факсом за адресами, вказаними у Договорі.
13.3. У випадку зміни адрес, банківських реквізитів, контактних телефонів тощо, вказаних у Договорі, Сторони зобов'язуються повідомляти про це іншу Сторону протягом 3 (трьох) робочих днів.
13.4. Обмін повідомленнями засобами електронної пошти у межах виконання умов цього Договору здійснюватиметься за наступними адресами (у разі, якщо письмово не будуть повідомлені інші адреси):

від Покупця: _____

від Постачальника: _____

## 14. ЮРИДИЧНІ АДРЕСИ та РЕКВІЗИТИ СТОРІН

Міністерство охорони здоров'я України

Адреса:
вул. М. Грушевського, 7,
м. Київ, 01601
Банківські реквізити Покупця:
Код ЄДРПОУ 00012925
IBAN UA 38 820172 0343161 0571 00000
199 в ДКСУ м. Київ
МФО 820172

Адреса:
Розрахунковий рахунок

_____
_____
_____
_____

## 14. ПЕРЕЛІК ДОДАТКІВ

Додаток 1: Умови постачання
Додаток 2: Технічні вимоги
Додаток 3: Шахрайство та корупція
Додаток 4: Заставне забезпечення авансового платежу Гарантія на вимогу

Засвідчуємо, що цей Договір підписано від імені Сторін вищевказаною датою:

**Від Покупця**

_____

_____

Заступник Міністра охорони здоров'я України

**Від Постачальника**

_____

**Додаток 1**
**до договору № HEAL-RFQ-4.1.1.9./___**
**від _____**

## УМОВИ НАДАННЯ ПОСЛУГ

*ТЕКСТ ВІДПОВІДНО ДО ЗАПОВНЕНОЇ ПОСТАЧАЛЬНИКОМ ФОРМИ*

**Додаток 2**
**до договору № HEAL-RFQ-4.1.1.9./___**
**від _____**

## ТЕХНІЧНІ ВИМОГИ

*ТЕКСТ ВІДПОВІДНО ДО ЗАПОВНЕНОЇ ПОСТАЧАЛЬНИКОМ ФОРМИ*

**Додаток 3**
**до договору № HEAL-RFQ-4.1.1.9./___**
**від _____**

## ШАХРАЙСТВО ТА КОРУПЦІЯ

### 1. Мета

1.1 Антикорупційні настанови Банку та це доповнення застосовуються до закупівель в рамках операцій Банку з фінансування інвестиційних проектів.

### 2. Вимоги

2.1 Банк вимагає від Позичальників (включаючи отримувачів фінансування від Банку); учасників торгів (тих, хто подав заявки/пропозиції), консультантів, підрядників та постачальників; будь-яких субпідрядників, субконсультантів, надавачів послуг або постачальників; будь-яких агентів (заявлених чи ні); та їх співробітників дотримуватись найвищих етичних стандартів під час процесу закупівель, відбору та виконання контрактів, що фінансуються Банком, та утримуватись від шахрайства та корупції.

2.2 З цією метою Банк:

a. Визначає, для цілей цього пункту, наведені нижче терміни таким чином:

i. “корупційні дії” – це пропонування, надання, отримання або вимагання, прямо чи опосередковано, будь-чого цінного з метою неналежного впливу на дії іншої сторони;

ii. “шахрайські дії” – це будь-які дії або бездіяльність, включаючи викривлення інформації, які навмисно або ненавмисно вводять в оману або намагаються ввести в оману сторону для отримання фінансової або іншої вигоди або уникнення виконання обов’язків;

iii. “дії щодо змови” – це домовленості між двома або більше сторонами, спрямовані на досягнення неналежної мети, включаючи неналежний вплив на дії іншої сторони;

iv. “дії щодо примушування” – це негативний вплив або завдання шкоди, або погрози негативно вплинути чи завдати шкоди, прямо чи опосередковано,

будь-якій стороні або її майну для здійснення неналежного впливу на дії сторони;

v. “перешкоджаючі дії” - це

(a) навмисне знищення, фальсифікація, зміна або приховування важливих для розслідування доказів або надання неправдивих заяв слідчим з метою суттєво завадити розслідуванню Банком звинувачень в корупційних або шахрайських діях, діях щодо змови або примушування, та/або погрози, домагання або залякування будь-якої сторони з метою недопущення розкриття нею відомостей, важливих для проведення розслідування, або подальшого проведення розслідування, або

(b) дії, спрямовані на суттєве перешкоджання реалізації Банком права на інспектування та аудит відповідно до пункту 2.2 e. нижче.

b. Відхиляє пропозицію щодо присудження контракту, якщо Банком буде з’ясовано, що рекомендований для укладання контракту консультант або його співробітники, агенти, субконсультанти, субпідрядники, надавачі послуг, постачальники та/або їх співробітники прямо чи опосередковано брали участь у корупційних або шахрайських діях, діях щодо змови або примушування або перешкоджаючих діях під час участі у конкурсі щодо зазначеного контракту;

c. На додаток до засобів правового захисту, визначених у відповідній угоді про позику, може вживати відповідні заходи, включаючи оголошення про порушення процедур закупівель, якщо Банком буде встановлено, що представники Позичальника або будь-якого з отримувачів будь-якої частини коштів Позики брали участь у корупційних або шахрайських діях, діях щодо змови або примушування або перешкоджаючих діях під час процесу відбору або виконання зазначеного контракту, і що Позичальником не було вжито своєчасних та належних заходів, що є задовільними на думку Банку, з метою реагування на такі дії на момент їх виникнення, включаючи відсутність своєчасного інформування Банку про такі дії;

d. Відповідно до Антикорупційних настанов Банку та згідно з поширеною на цей час санкційною політикою та процедурами Банку, може застосувати санкції до фірми або фізичної особи на невизначений або визначений період часу, включаючи публічне оголошення про позбавлення такої фірми або фізичної особи права: (i) на присудження контракту, що фінансується Банком, або отримання від нього будь-якої фінансової чи іншої вигоди[2]; (ii) на пропонування[3] в якості субпідрядника, консультанта, виробника, постачальника або надавача послуг іншої фірми, яка має право на присудження контракту, що фінансується Банком; та (iii) на отримання коштів в рамках будь-якої позики, наданої Банком, або на будь-яку подальшу участь у підготовці або реалізації проекту, що фінансується Банком;

e. Вимагає включення до тендерної документації/запитом до надання пропозицій та до контрактів, що фінансуються за рахунок позики Банку, вимоги до учасників (тих, хто подає заявки/пропозиції), консультантів, підрядників та постачальників, їх субпідрядників,

[2] Для уникнення сумнівів, позбавлення сторони, до якої застосовано санкції, права на присудження контракту має поширюватись, без обмежень, на (i) подання заявки на передкваліфікацію, висловлення інтересу в наданні консультаційних послуг та подання заявок, прямо чи в якості пропонованого субпідрядника, пропонованого консультанта, пропонованого виробника або постачальника або номінованого надавача послуг щодо цього контракту, та (ii) внесення доповнень або змін, що спричиняють суттєву модифікацію існуючого контракту.

[3] Пропонований субпідрядник, пропонований консультант, пропонований виробник або постачальних або пропонований надавач послуг (використовуються різні назви в залежності від конкретної тендерної документації) це той, хто був (i) включений консультантом до передкваліфікаційної заявки через специфічний та надзвичайно важливий досвід та ноу-хау, що забезпечують відповідність учасника кваліфікаційним вимогам за конкретною заявкою; або (ii) призначений Позичальником.

субконсультантів, надавачів послуг, постачальників, агентів дозволити Банку інспектувати[4] всі рахунки, записи та інші документи, що стосуються процесу закупівель, відбору та/або виконання контракту, а також дозволити їх аудит призначеними Банком аудиторами

[4] У цьому контексті інспекції носять слідчий характер (експертиза). Вони включають заходи із встановлення фактів, що вживаються Банком або особами, призначеними Банком, для реагування на конкретні питання, що стосуються розслідувань/аудитів, як то оцінка правдивості звинувачень у можливому шахрайстві та корупції, шляхом використання належних механізмів. Така діяльність включає, не обмежуючись: доступ та огляд фінансової документації та інформації фірми або фізичної особи, зняття копій у разі необхідності; доступ та огляд будь-яких інших документів, даних та інформації (у паперовому або електронному вигляді), що вважаються важливими для розслідування/аудиту, та зняття копій у разі необхідності; опитування співробітників та інших відповідних осіб; здійснення фізичних інспекцій та виїздів на місце; отримання підтверджень інформації з боку третіх осіб.

**Додаток 4**
**до договору № HEAL-RFQ-4.1.1.9./___**
**від _____**

**Заставне забезпечення авансового платежу**

**Гарантія на вимогу**

*[на прохання переможця, банк заповнює цю форму згідно з наведеними інструкціями]*

*[офіційний бланк Гаранта або ідентифікаційний код SWIFT]*

**Бенефіціар:** [*вказати назву та адресу Покупця*]

**Дата:** *[вказати дату випуску]*

**Гарантія повернення авансового платежу №:***[вказати номер гарантії]*

**Гарант:** *[вказати назву та адресу місця випуску, окрім випадків, коли вони вказані на офіційному бланку]*

Ми отримали інформацію про те, що *[вказати повну назву Постачальника (у випадку ОП – назву ОП)]* (далі – «Заявник») уклав Договір № *[вказати номер Договору]* від *[вказати дату та місяць], [рік]* з Бенефіціаром на постачання *[опис товарів та відповідних послуг]* (далі – «Договір»).

Крім того, ми розуміємо, що відповідно до умов Договору авансовий платіж у сумі [*вказати суму цифрами і прописом*] здійснюється проти гарантії повернення авансового платежу.

На прохання Заявника цим документом ми, як Гарант, цим безвідклично зобов'язуємося сплатити Бенефіціару будь-яку(і) суму(и), що не перевищує(ють) [*вкажіть суму(и) цифрами та словами*][5] після отримання нами першої письмової вимоги Бенефіціара, підтвердженої його заявою (у складі самої вимоги чи в окремому підписаному документі, який супроводжує або визначає цю вимогу) про те, що Заявник:

(a) використав авансовий платіж для інших потреб, ніж постачання Товарів; або

(b) не повернув авансовий платіж відповідно до умов Договору, вказавши суму, яку Заявник не повернув.

Умовою подання будь-якої вимоги за цією Гарантією є представлення Гаранту довідки з банку Бенефіціара, яка підтверджує отримання Заявником авансового платежу, про який йдеться вище, на свій рахунок [*вставте номер рахунка, назву і адресу банку Заявника*].

Максимальна сума цієї гарантії буде поступово зменшуватися на суму авансового платежу, погашеного заявником, як зазначено в копіях проміжних виписок або платіжних сертифікатів, які мають бути представлені нам. Ця гарантія втрачає чинність не пізніше, як після отримання нами копії сертифіката проміжного платежу, в якому зазначено, що

[5] *Гарант має вказати суму, яка представляє суму авансового платежу і виражена або у у валюті (валютах) авансового платежу Договору або у будь-якій іншій вільно конвертованій валюті, прийнятній для Покупцяю*

дев'яносто (90) відсотків прийнятої вартості Договору було підтверджено до оплати, або в день [*вкажіть день*] [*вкажіть місяць*], [*вкажіть рік*], залежно від того, яка з них настане раніше. Отже, будь-яка вимога на оплату за цією гарантією має бути отримана нами в цьому офісі на цю дату або до неї.

Ця Гарантія регулюється Загальними правилами щодо Гарантій на вимогу (Uniform Rules for Demand Guarantees (URDG) 2010 ), вісник No. 758 Міжнародної торгової палати 758 за винятком обгрунтовувальної заяви зі Статті 15(a), яку цим вилучено.

_____
*[підписи]*

***Примітка: Вест текст поданий курсивом, включаючи примітки, наведений для потреб підготовки цієї форми і має бути вилучений з остаточної версії продукту.***