

Додаток 6
до Пріоритетної тематики, за якою
здійснюватиметься державне замовлення
на найважливіші науково-технічні
(експериментальні) розробки та науково-
технічну продукцію у 2027–2028 роках
(пункт 6)

ВИХІДНЕ ТЕХНІЧНЕ ЗАВДАННЯ **НА ВИКОНАННЯ НАУКОВО-ТЕХНІЧНОЇ (ЕКСПЕРИМЕНТАЛЬНОЇ) РОЗРОБКИ**

1. Назва науково-технічної (експериментальної) розробки (далі – Розробка):

(заповнюється учасником Конкурсу)

2. Назва пріоритетної тематики, за якою здійснюватиметься державне замовлення на найважливіші науково-технічні (експериментальні) розробки та науково-технічну продукцію у 2027-2028 роках (згідно з переліком, затвердженим наказом МОН)

Розроблення локальної платформи штучного інтелекту для автоматизованого дослідження та аналізу шкідливого програмного забезпечення.

3. Мета і вихідні дані для виконання Розробки

3.1. Мета виконання Розробки

Метою виконання Розробки є розроблення програмної платформи локального розгортання із застосуванням технологій штучного інтелекту для підтримки процесів автоматизованого дослідження та технічного аналізу шкідливого програмного забезпечення (далі – Платформа).

3.2. Проблеми, на вирішення яких має бути спрямована Розробка

Проблеми, які вирішує Платформа:

висока трудомісткість і тривалість автоматизованого дослідження шкідливого програмного забезпечення, зумовлені значним обсягом ручного опрацювання коду, бінарних структур, функцій, викликів, текстових рядків, ділянок пам'яті та інших об'єктів дослідження;

фрагментарність інструментів і результатів аналізу, що ускладнює узагальнення результатів статичного та динамічного аналізу, навігацію між пов'язаними об'єктами та формування цілісного уявлення про поведінку зразка шкідливого програмного забезпечення;

складність семантичного аналізу декомпільованого коду, зокрема встановлення призначення функцій, відновлення логіки алгоритмів, уточнення типів даних, перейменування сутностей і визначення взаємозв'язків між компонентами;

відсутність автоматизованої підтримки пріоритизації дослідження, через що профільний фахівець-аналітик (далі — Користувач) змушений вручну визначати функції, ділянки коду, технічні ознаки та поведінкові характеристики, які мають найбільше аналітичне значення;

залежність повноти та якості результатів від досвіду окремого Користувача, а також недостатня стандартизація підходів до аналізу, опису поведінки, фіксації результатів і підготовки звітних матеріалів;

складність виявлення схожих, повторно використаних або модифікованих фрагментів коду, спільних поведінкових характеристик і зв'язків із відомими зразками чи сімействами шкідливого програмного забезпечення;

недостатнє повторне використання накопичених знань, пов'язане з розрізненим зберіганням результатів попередніх досліджень, пояснень, індикаторів компрометації, поведінкових характеристик і аналітичних висновків;

висока трудомісткість підготовки захисних та аналітичних матеріалів, зокрема індикаторів компрометації, сигнатур виявлення, правил YARA і Sigma, рекомендацій та структурованих технічних звітів;

недостатня простежуваність і відтворюваність результатів, зумовлена відсутністю системного зв'язку висновків із конкретними технічними даними, а також належної реєстрації вхідного контексту, викликів модулів і моделей штучного інтелекту, їх версій, параметрів виконання, сформованих результатів та етапів їх перевірки Користувачем;

ризик використання неперевіраних результатів, сформованих засобами штучного інтелекту, що зумовлює необхідність чіткого розмежування статусів таких результатів — «сформовано Платформою», «потребує уточнення», «перевірено Користувачем», «затверджено Користувачем» і «відхилено Користувачем» — та збереження визначальної ролі Користувача;

ризик витоку або неконтрольованого передавання досліджуваних даних, що зумовлюють необхідність локального розгортання та функціонування Платформи в межах дозволеного захищеного контуру Замовника без передавання таких даних до інформаційних систем і сервісів за межами цього контуру;

недостатня масштабованість ручних процесів аналізу в умовах зростання кількості, складності та різноманітності зразків шкідливого програмного забезпечення.

3.3. Вихідні дані для розроблення науково-технічної продукції (у разі необхідності)

Закон України «Про захист інформації в інформаційно-комунікаційних системах»;

постанова Кабінету Міністрів України від 29 березня 2006 р. № 373 «Про затвердження Мінімальних вимог до захисту інформаційних, електронних комунікаційних, інформаційно-комунікаційних та технологічних систем»;

постанова Кабінету Міністрів України від 21 лютого 2025 р. № 205 «Деякі питання створення, адміністрування та забезпечення функціонування засобу інформатизації»;

наказ Адміністрації Держспецзв'язку від 30 січня 2026 р. № 75 «Про затвердження Каталогу заходів з кіберзахисту, базових заходів з кіберзахисту, форми плану кіберзахисту та методичних рекомендацій щодо здійснення заходів з кіберзахисту»;

наказ Адміністрації Держспецзв'язку від 23 лютого 2026 р. № 154 «Про затвердження Рекомендацій з кіберзахисту інформаційно-комунікаційних систем, які використовують технології штучного інтелекту»;

ДСТУ ISO/IEC/IEEE 29148:2025 Інженерія систем і програмних засобів. Процеси життєвого циклу. Інженерія вимог (ISO/IEC/IEEE 29148:2018, IDT);

ДСТУ ISO/IEC 25010:2025 Інженерія систем і програмних засобів. Вимоги до якості систем і програмних засобів та її оцінювання (SQuaRE). Модель якості продукту (ISO/IEC 25010:2023, IDT);

ДСТУ ISO/IEC/IEEE 15289:2025 Інженерія систем і програмних засобів. Уміст інформаційних об'єктів життєвого циклу (ISO/IEC/IEEE 15289:2019, IDT);

ДСТУ ISO/IEC/IEEE 29119-2:2017 Інженерія систем і програмних засобів. Тестування програмних засобів. Частина 2. Процеси тестування (ISO/IEC/IEEE 29119-2:2013, IDT);

ДСТУ ISO/IEC TR 27563:2024 Безпека та конфіденційність у разі застосування штучного інтелекту. Передові практики (ISO/IEC TR 27563:2023, IDT);

ДСТУ ISO/IEC/IEEE 42010:2025 Програмні засоби, системи та підприємство. Опис архітектури (ISO/IEC/IEEE 42010:2022, IDT).

Інформація, яка є необхідною для виконання Розробки, але є відсутньою у відкритому доступі, буде надана Виконавцю за запитом через Замовника в установленому порядку.

4. Основні характеристики науково-технічної продукції, яку буде створено за результатами виконання Розробки

4.1. Опис науково-технічної продукції, яка буде створена в результаті виконання Розробки, її функціональне призначення

У результаті виконання Розробки має бути виготовлено дослідний зразок програмної платформи локального розгортання із застосуванням технологій штучного інтелекту для підтримки процесів автоматизованого дослідження та технічного аналізу шкідливого програмного забезпечення.

Платформа призначена для автоматизації, прискорення та стандартизації основних етапів дослідження зразків шкідливого програмного забезпечення, інтегрованого опрацювання результатів статичного й динамічного аналізу, семантичного аналізу програмного коду, пошуку схожості, формування захисних артефактів, накопичення результатів попередніх досліджень і підготовки структурованих аналітичних матеріалів.

Платформа має забезпечувати інтегроване застосування засобів та технологій штучного інтелекту, автоматизацію, прискорення і стандартизацію основних етапів аналізу — від попереднього профілювання зразків до пояснення логіки функцій, пошуку схожості, формування захисних артефактів і структурованих аналітичних звітів.

Платформа має виконувати допоміжну функцію та підвищувати ефективність роботи Користувача, а також забезпечувати простежуваність і відтворюваність результатів. Експертна оцінка, перевірка та остаточне затвердження результатів здійснюються Користувачем. Створена Платформа має бути придатною до розгортання, демонстрації та дослідної експлуатації в локальній інфраструктурі організації, яка буде використовувати Платформу.

Платформа має будуватися за модульним принципом і включати такі основні функціональні підсистеми:

- підсистему інтеграції з інструментами автоматизованого дослідження та отримання даних про об'єкти дослідження;

- підсистему попереднього профілювання зразків шкідливого програмного забезпечення;

- підсистему семантичного аналізу програмного коду;

- підсистему виявлення поведінкових характеристик і технік протидії аналізу;

- підсистему пошуку схожості та класифікації зразків;

- підсистему формування захисних артефактів;

- підсистему формування технічних і аналітичних звітів;

- підсистему накопичення, пошуку та повторного використання результатів попередніх досліджень;

- підсистему керування процесом аналізу, перевірки та простежуваності результатів;

- підсистему взаємодії з Користувачем;

- підсистему адміністрування, захисту, журналювання та моніторингу.

Підсистема інтеграції з інструментами автоматизованого дослідження та отримання даних про об'єкти дослідження має забезпечувати керований обмін даними між Платформою та зовнішніми програмними засобами аналізу. Обміну підлягають відомості про функції, графи викликів функцій, імпортовані компоненти, текстові рядки, перехресні посилання, ділянки пам'яті, послідовності байтів, бінарні структури, інструкції, базові блоки, декомпільований код та інші доступні об'єкти дослідження. Платформа має забезпечувати інтеграцію з Ghidra версії 12.1.2 або новішої сумісної версії, IDA Pro версії 9.4 або новішої сумісної версії та x64dbg версії 2026.05.27 або новішої сумісної версії. Сумісність із новішими версіями має підтверджуватися результатами інтеграційних випробувань. Інтеграція з Ghidra та IDA Pro має забезпечувати отримання та контрольоване внесення даних про функції, графи викликів, імпортовані компоненти, текстові рядки, перехресні посилання, типи даних, сигнатури функцій, коментарі, декомпільований код і послідовності байтів. Інтеграція з x64dbg має забезпечувати отримання результатів динамічного аналізу, зокрема відомостей про виконання функцій, виклики програмних інтерфейсів, завантажені модулі, потоки, ділянки пам'яті та зміни стану досліджуваного процесу. Інтеграція зі сторонніми програмними продуктами здійснюється за

наявності належних ліцензій і відповідно до умов їх використання. Підсистема інтеграції з інструментами автоматизованого дослідження та отримання даних про об'єкти дослідження має підтримувати взаємодію із зовнішніми інструментами та сервісами через стандартизовані програмні інтерфейси, зокрема сервери протоколу Model Context Protocol (далі — MCP-сервери), для контрольованого отримання даних і виконання дозволених операцій. Підсистема інтеграції з інструментами автоматизованого дослідження та отримання даних про об'єкти дослідження має підтримувати отримання результатів аналізу та контрольоване передавання до проєкту автоматизованого дослідження затверджених Користувачем коментарів, найменувань функцій і змінних, типів даних, сигнатур функцій, міток та інших результатів семантичного аналізу програмного коду. Усі зміни мають реєструватися та мати можливість скасування.

Підсистема попереднього профілювання зразків має забезпечувати визначення формату файлу, цільової платформи й архітектури, витяг метаданих, імпортованих компонентів, текстових рядків та індикаторів компрометації, виявлення ознак пакування, обфускації й протидії аналізу, а також визначення об'єктів, що мають пріоритетне аналітичне значення.

Попереднє профілювання має здійснюватися на основі доступних статичних даних і результатів контрольованого динамічного аналізу. Підсистема має формувати попередні припущення щодо наявності у зразку функціональних компонентів, пов'язаних із мережевою взаємодією, шифруванням або розшифруванням даних, виконанням команд, закріпленням у системі, ін'єкцією у процеси, викраденням інформації, протидією аналізу та іншими потенційно шкідливими можливостями. Кожне припущення має містити посилання на технічні дані, на яких воно ґрунтується.

Підсистема семантичного аналізу програмного коду має забезпечувати функціональне групування й класифікацію функцій за їх імовірним призначенням, визначення пріоритетних об'єктів дослідження, підготовку стислих описів функцій і ланцюгів їх викликів, пояснення логіки роботи декомпільованого коду та взаємозв'язків між його компонентами.

Підсистема має підтримувати формування запитів щодо функцій, текстових рядків, імпортованих компонентів, перехресних посилань та інших об'єктів аналізу, а також підготовку пропозицій щодо найменування функцій і змінних, визначення типів даних, уточнення сигнатур функцій, додавання коментарів і покращення читабельності декомпільованого коду.

Покращення читабельності декомпільованого коду може охоплювати узгодження найменувань, пояснення складних конструкцій, узагальнення повторюваних шаблонів, зменшення надлишкового представлення та відновлення ймовірного змістового призначення окремих елементів. Запропоновані за результатами семантичного аналізу зміни найменувань, типів даних, сигнатур функцій, коментарів та інших елементів представлення не повинні змінювати фактичну логіку досліджуваного коду або підміняти результати спеціалізованих засобів дизасемблювання та декомпіляції.

Підсистема виявлення поведінкових характеристик і технік протидії аналізу має забезпечувати встановлення поведінкових характеристик досліджуваного зразка, пов'язаних із мережевою взаємодією, криптографічними операціями, виконанням команд, закріпленням у системі, ін'єкцією у процеси, викраденням облікових даних та іншими функціональними можливостями.

Підсистема має також забезпечувати виявлення технічних ознак пакування, обфускації, прихованого використання програмних інтерфейсів, протидії налагодженню, протидії виконанню у віртуальному середовищі та інших технік, що ускладнюють аналіз.

Підсистема пошуку схожості та класифікації зразків має забезпечувати порівняння функцій, базових блоків, фрагментів коду, бінарних структур, текстових рядків і поведінкових характеристик із результатами попередніх досліджень та еталонними даними. Пошук схожості має підтримувати виявлення повторного використання коду, модифікованих реалізацій

відомих алгоритмів, споріднених версій зразків і можливих зв'язків між сімействами шкідливого програмного забезпечення. Підсистема має забезпечувати попередню класифікацію зразків за типом шкідливого програмного забезпечення, ймовірною належністю до відомого сімейства, функціональними можливостями, цільовою платформою, архітектурою та іншими визначеними класами. Класифікація має здійснюватися на основі встановлених технічних і поведінкових характеристик, результатів пошуку схожості та еталонних даних. Результати пошуку схожості та класифікації мають містити об'єкти порівняння, використані ознаки, запропонований клас або сімейство, оцінку ступеня схожості та рівня впевненості, а також конкретні технічні дані, що обґрунтовують сформований результат. Попередня класифікація та встановлення належності зразка до конкретного сімейства підлягають обов'язковій перевірці й затвердженню Користувачем.

Підсистема формування захисних артефактів має забезпечувати підготовку проєктів індикаторів компрометації, сигнатур виявлення, правил YARA, правил Sigma та інших засобів виявлення. Захисні артефакти мають формуватися на основі зафіксованих результатів технічного аналізу, бути пов'язаними з відповідними об'єктами дослідження та підлягати обов'язковій перевірці Користувачем.

Підсистема формування технічних і аналітичних звітів має забезпечувати підготовку структурованих технічних звітів, проміжних узагальнень і стислих аналітичних резюме за уніфікованими шаблонами. Сформовані матеріали мають містити відомості про досліджений зразок, установлені функціональні та поведінкові характеристики, індикатори компрометації, виявлені зв'язки, підготовлені захисні артефакти, статуси перевірки результатів і технічні дані, на яких ґрунтуються висновки.

Підсистема накопичення, пошуку та повторного використання результатів попередніх досліджень має забезпечувати централізоване зберігання даних про досліджені зразки, їх контрольні суми, функції, фрагменти коду, текстові рядки, поведінкові характеристики, пояснення, висновки, індикатори компрометації, захисні артефакти та встановлені зв'язки. Підсистема має підтримувати пошук за структурованими атрибутами та семантичними ознаками, а також контрольоване використання результатів попередніх досліджень як додаткового контексту під час аналізу нових зразків. Конкретні технології зберігання, індексування, побудови векторних представлень і пошуку визначаються під час проєктування Платформи.

Підсистема керування процесом аналізу, перевірки та простежуваності результатів має забезпечувати ведення окремих досліджень, розподіл завдань, визначення стану опрацювання, збереження історії дій та зв'язок сформованих результатів із конкретними об'єктами дослідження. Для результатів аналізу мають застосовуватися статуси, що відображають стан їх формування, перевірки та подальшого використання:

«сформовано Платформою» — результат автоматично сформований Платформою та ще не перевірений Користувачем; такий результат має попередній характер і не може використовуватися як затверджений висновок;

«потребує уточнення» — Користувач або Платформа встановили недостатність, неоднозначність чи суперечливість технічних даних, унаслідок чого результат потребує додаткового аналізу, доповнення або повторного опрацювання;

«перевірено Користувачем» — Користувач перевірів технічні дані, джерела, логічні зв'язки та обґрунтування результату й визнав їх достатніми для подальшого використання або підготовки остаточного висновку;

«затверджено Користувачем» — Користувач остаточно схвалив результат і дозволив його використання у технічних та аналітичних звітах, захисних артефактах, проєктах автоматизованого дослідження або передавання до інтегрованих інформаційних систем відповідно до наданих повноважень;

«відхилено Користувачем» — Користувач визнав результат помилковим, недостатньо обґрунтованим, нерелевантним або непридатним для подальшого використання.

Платформа має зберігати історію зміни статусів, дату й час кожної зміни, ідентифікатор Користувача, який виконав дію, підставу зміни статусу та зв'язок із відповідними технічними даними. Перехід до статусів «перевірено Користувачем», «затверджено Користувачем» і «відхилено Користувачем» має здійснюватися виключно уповноваженим Користувачем. Для забезпечення простежуваності та відтворюваності результатів Платформа має реєструвати використані вхідні дані та їх контрольні суми, контекст аналізу, версії програмних модулів і моделей штучного інтелекту, параметри виконання, сформовані результати, дії Користувача та зв'язок висновків із конкретними функціями, текстовими рядками, викликами, перехресними посиланнями, ділянками пам'яті або фрагментами коду.

Підсистема взаємодії з Користувачем має забезпечувати вебінтерфейс для доступу до функціональних можливостей Платформи, перегляду й навігації між об'єктами дослідження, формування запитів, перевірки результатів, затвердження запропонованих змін і підготовки аналітичних матеріалів. Платформа має підтримувати паралельне опрацювання кількох зразків або окремих сеансів аналізу з розмежуванням їх даних, результатів і журналів дій. Платформа має забезпечувати прикладний програмний інтерфейс (API) для взаємодії між її компонентами, інтеграції із зовнішніми програмними засобами та інформаційними системами, а також автоматизованого доступу до її функціональних можливостей.

Підсистема адміністрування, захисту, журналювання та моніторингу має забезпечувати керування конфігурацією Платформи, автентифікацію Користувача, розмежування повноважень, реєстрацію подій і дій, контроль стану програмних компонентів, резервне копіювання, відновлення та інші необхідні експлуатаційні функції.

Результати, сформовані із застосуванням технологій штучного інтелекту, до їх перевірки та затвердження Користувачем мають попередній характер. Платформа повинна забезпечувати відокремлення встановлених фактів від припущень, відображення рівня впевненості та посилання на конкретні технічні дані, на яких ґрунтується результат.

Платформа може формувати проєкти аналітичних гіпотез і попередні оцінки. Їх перевірка, уточнення, підтвердження та остаточне затвердження здійснюються Користувачем.

Платформа не повинна самостійно надавати аналітичним висновкам статус «затверджено Користувачем», остаточно встановлювати належність зразка, публікувати захисні артефакти, вносити незворотні зміни до проєкту автоматизованого дослідження або виконувати програмний код, сценарії чи команди, сформовані засобами штучного інтелекту.

Платформа має розгортатися на обчислювальних ресурсах органу, яким було заявлено зазначену пріоритетну тематику та сформовано відповідне вихідне Технічне завдання, та функціонувати в межах локального захищеного контуру. Зразки шкідливого програмного забезпечення, декомпільований код, результати аналізу, сформовані артефакти та інші досліджувані дані не повинні передаватися до зовнішніх сервісів.

Базові налаштування безпеки та контролю доступу мають передбачати:

- автентифікацію Користувача;
- рольове розмежування повноважень відповідно до принципу мінімально необхідних прав;
- розмежування адміністративних та аналітичних функцій;
- захист облікових даних, ключів доступу та інших секретів;
- обмеження мережевої взаємодії межами дозволеного локального контуру;
- захищену взаємодію між компонентами Платформи;
- реєстрацію входів, адміністративних дій, операцій із досліджуваними зразками та змін результатів аналізу;
- захист журналів від несанкціонованого видалення або зміни;
- контроль цілісності конфігурацій і критичних програмних компонентів;
- ізоляцію середовищ контрольованого динамічного аналізу зразків;

блокування неконтрольованого передавання досліджуваних даних до зовнішніх інформаційних ресурсів;

безпечне резервне копіювання та відновлення;

можливість зміни початкових параметрів безпеки відповідно до вимог органу, яким було заявлено зазначену пріоритетну тематику та сформовано відповідне вихідне Технічне завдання.

Під час виконання Розробки мають бути проведені випробування дослідного зразка Платформи, результати яких оформлюються комплектом випробувальної документації та матеріалів випробування, а саме:

функціональні випробування;

інтеграційні випробування;

випробування встановлення, оновлення, резервного копіювання та відновлення;

навантажувальні випробування;

перевірку механізмів захисту;

перевірку стійкості до некоректних даних;

оцінювання модулів штучного інтелекту;

демонстрацію функціональних можливостей Платформи в локальному ізольованому випробувальному середовищі, що забезпечує функціонування передбачених цим технічним завданням компонентів і проведення встановлених видів випробувань.

Оцінювання модулів штучного інтелекту має здійснюватися за наступними критеріями:

правильність отримання технічних даних та індикаторів компрометації;

правильність функціонального групування і класифікації функцій та зразків;

якість визначення пріоритетних об'єктів дослідження;

правильність і обґрунтованість пояснення призначення функцій, алгоритмів та взаємозв'язків між компонентами;

якість пошуку схожості та виявлення повторного використання коду;

правильність визначення поведінкових характеристик і технік протидії аналізу;

якість сформованих пропозицій щодо найменувань, типів даних, сигнатур функцій і коментарів;

якість проєктів захисних артефактів;

правильність і повнота сформованих технічних та аналітичних матеріалів;

простежуваність результатів до конкретних технічних даних.

Первинне інформаційно-аналітичне наповнення Платформи має включати:

шаблони технічних та аналітичних звітів;

шаблони і приклади захисних артефактів, зокрема індикаторів компрометації, сигнатур виявлення, правил YARA, правил Sigma та інших засобів виявлення;

базові довідники, словники, класифікатори й таксономії;

початкові набори тестових, демонстраційних та еталонних даних, зокрема для перевірки пошуку схожості та повторного використання результатів попередніх досліджень;

початкові налаштування моделей, алгоритмів, правил і параметрів аналізу;

приклади результатів аналізу контрольних зразків.

4.2. Відповідність рівню технологічної готовності (Technology Readiness Levels), який пропонується досягнути в Розробці у порівнянні з необхідним (не нижче TRL4 та не вище TRL7 (TRL8 - для програмних продуктів):

TRL7 - здійснено випуск прототипу, технологію (розробку) успішно продемонстровано у робочому середовищі.

Для досягнення зазначеного TRL Виконавцю Розробки буде надано допомогу з боку органу, яким надано пропозиції до пріоритетної тематики та сформовано вихідне Технічне завдання на виконання Розробки, у проведенні таких робіт: тестуванні програмного продукту в робочому середовищі (зокрема, на базі серверних потужностей цього органу), наданні

необхідних дозволів, підписанні протоколів за результатами проведення тестування (випробувань).

4.3. Відповідність рівня технологічної готовності (TRL*), який буде досягнуто в результаті виконання Розробки, рівню технологічної готовності, який зазначено в Технічному завданні, наданому міністерством, іншим центральним органом виконавчої влади.

(заповнюється учасником Конкурсу)

TRL, який необхідний згідно вимог	TRL, який пропонується
TRL7	(заповнюється учасником Конкурсу)

*Вводиться відповідний рівень технологічної готовності:

TRL1 - сформульовано базові принципи технології (розробки);

TRL2 - сформульовано концепцію технології (розробки);

TRL3 - проведено першу оцінку ефективності застосування ідеї і технології, концепцію технології (розробки) доведено експериментально;

TRL4 - технологію (розробку) перевірено в лабораторних умовах;

TRL5 - технологію (розробку) перевірено у відповідному (промисловому) середовищі

TRL6 - здійснено випуск дослідного зразка, технологію (розробку) успішно продемонстровано у відповідному (промисловому) середовищі;

TRL7 - здійснено випуск прототипу, технологію (розробку) успішно продемонстровано у робочому середовищі;

TRL8 - виробництво з використанням технології (розробки) повністю перевірене, затверджене і готове до запуску;

TRL9 - запуск серійного виробництва з використанням технології (розробки).

4.4. Відповідність основним очікуваним характеристикам науково-технічної продукції та вимогам до неї:

Характеристики* (зазначити необхідні):				
Тип	Назва характеристики/вимоги, її короткий опис	Діапазон потрібних значень	Чим регламентується (ДСТУ, інші стандарти тощо (за наявності))	Діапазон значень, які будуть досягнуті в результаті Розробки
технічні (тактико-технічні)	Локальна програмна платформа для автоматизованого статичного та динамічного аналізу шкідливого програмного забезпечення з використанням методів штучного інтелекту	Підтримка аналізу виконуваних файлів, скриптів, бібліотек ОС Windows, Linux, macOS, мобільних Android додатків, офісних файлів. Статичний та динамічний аналіз		
експлуатаційні	Експлуатація в умовах захищеного операційного	Цілодобова робота (24/7)		

	середовища із можливістю інтеграції окремих елементів до хмарних рішень.			
фізико-хімічні				
механічні				
якісні	Точність автоматизованої класифікації та ідентифікації шкідливого програмного забезпечення	Зменшення часу дослідження зразку на 60% у порівнянні із ручним аналізом		
споживчі				
інші	Можливість інтеграції з наявними засобами кіберзахисту, збагачення даних, платформ кіберрозвідки органу, яким було заявлено зазначену пріоритетну тематику та сформовано відповідне вихідне Технічне завдання, профільними хмарними сервісами, плагінами, інструментами реверс інжинірингу			
Вимоги* (зазначити необхідні):				
медичні (клінічні)	Захист від несанкціонованого доступу, ізоляція середовища аналізу, захист прав доступу для унеможливлення виходу зразка за межі операційного середовища			
вимоги до надійності / захищеності	Робота на серверному обладнанні органу, яким було заявлено зазначену пріоритетну тематику та сформовано відповідне вихідне Технічне завдання	Сумісність з типовими x86_64 серверами		
вимоги до потужності	Аналіз та дослідження шкідливого програмного забезпечення			
вимоги щодо призначеності	Оптимізоване використання обчислювальних ресурсів			
вимоги щодо ресурсо- та енергозбереження	Захист від несанкціонованого доступу, ізоляція середовища аналізу			

вимоги до технологічності	Модульна архітектура, можливість оновлення та розширення функціоналу			
вимоги безпеки	Виключення впливу досліджуваного шкідливого ПЗ на продуктивне середовище			
конструктивні				
вимоги щодо ергономіки та технічної естетики	Зрозумілий інтерфейс користувача, орієнтований на фахівців з кібербезпеки			
вимоги охорони довкілля, утилізація				
спеціальні вимоги (в тому числі на вимогу замовника)				
інші				
Необхідні вимоги до умов експлуатації (за наявності)*:				
вимоги щодо безпеки під час транспортування та зберігання (забезпечення збереженості) продукції				
вимоги щодо експлуатації та ремонту, дотримання яких забезпечує працездатність і безпечність продукції та гарантує спожиткові (експлуатаційні) характеристики				
інші				

* **Примітка:** зазначаються залежно від виду та призначення НТП.

5. Результати виконання Розробки та їх відповідність пріоритетним державним потребам:

5.1. Інформація про науково-технічну продукцію, що буде створена і передана в результаті виконання Розробки.

В результаті виконання Розробки буде створена та передана Замовнику наступна науково-технічна продукція:

1) програмне забезпечення Платформи, до складу якого мають входити:

серверна частина для приймання, зберігання й опрацювання зразків та пов'язаних із ними даних (виконання зразків допускається лише в ізольованому середовищі контрольованого динамічного аналізу);

засоби інтеграції з інструментами автоматизованого дослідження, зокрема Ghidra, IDA Pro та x64dbg, а також із MCP-серверами;

засоби отримання, нормалізації та опрацювання результатів статичного й динамічного аналізу;

засоби попереднього профілювання зразків, витягу метаданих, текстових рядків, імпортованих компонентів та індикаторів компрометації;

модулі штучного інтелекту для семантичного аналізу декомпільованого коду, пояснення призначення функцій, алгоритмів і взаємозв'язків між компонентами;

засоби функціонального групування, класифікації та визначення пріоритетних об'єктів подальшого дослідження;

засоби підготовки пропозицій щодо найменування функцій і змінних, визначення типів даних, уточнення сигнатур функцій, коментування та покращення читабельності декомпільованого коду;

засоби виявлення поведінкових характеристик, технічних ознак пакування й обфускації, а також технік протидії аналізу;

засоби пошуку схожості між функціями, фрагментами коду, бінарними структурами, поведінковими характеристиками та дослідженими раніше зразками;

засоби формування проєктів захисних артефактів, зокрема індикаторів компрометації, сигнатур виявлення, правил YARA, правил Sigma та інших засобів виявлення;

засоби формування проміжних узагальнень, структурованих технічних звітів і стислих аналітичних резюме;

засоби накопичення, пошуку та повторного використання результатів попередніх досліджень;

засоби керування процесом аналізу, статусами перевірки, простежуваністю та відтворюваністю результатів;

вебінтерфейс для взаємодії Користувачів із Платформою, перегляду об'єктів дослідження, формування запитів, перевірки результатів і виконання інших передбачених функцій;

прикладний програмний інтерфейс (API) для взаємодії між компонентами Платформи, інтеграції із зовнішніми програмними засобами та інформаційними системами, а також автоматизованого доступу до функціональних можливостей Платформи;

засоби адміністрування, керування доступом, журналювання, моніторингу, резервного копіювання та відновлення;

бази даних, файлові сховища, пошукові індекси та інші програмні компоненти, необхідні для функціонування Платформи;

2) комплект вихідних програмних матеріалів Платформи має включати:

вихідний програмний код компонентів, розроблених у межах Розробки;

схеми баз даних і сценарії їх міграції;

конфігураційні файли та шаблони конфігурації, необхідні для складання Платформи з вихідного програмного коду;

програмні адаптери та інтеграційні компоненти;

програмний код автоматизованих тестів;

сценарії складання та підготовки випуску Платформи;

перелік програмних залежностей, сторонніх бібліотек, моделей, програмних продуктів та інших компонентів із зазначенням їх версій, походження, умов ліцензування;

файли моделей штучного інтелекту або засоби їх контрольованого отримання та встановлення;

3) Інструкція зі створення готової до встановлення версії Платформи з вихідного програмного коду;

4) комплект засобів розгортання та налаштування Платформи має включати:

інсталяційні пакети або образи програмних компонентів;

сценарії автоматизованого встановлення, первинного налаштування, оновлення, резервного копіювання, перевірки резервних копій, відновлення та видалення Платформи;

конфігурації серверних компонентів, баз даних, сховищ, моделей штучного інтелекту та інтеграційних модулів;
 шаблони параметрів середовища без облікових даних, ключів доступу та інших секретів;
 засоби перевірки готовності середовища та працездатності компонентів;
 базову конфігурацію журналювання, моніторингу та сповіщення про порушення в роботі Платформи;

конфігурації мережевої взаємодії, необхідні для функціонування Платформи в локальному контурі;

5) комплект технічної, експлуатаційної та методичної документації має включати:
 технічний опис Платформи, її призначення, архітектури, функціональних підсистем, програмних компонентів, інформаційних потоків і взаємодії із зовнішніми інструментами;
 опис вимог до апаратного і програмного забезпечення;
 опис форматів вхідних і вихідних даних;
 опис структури баз даних, файлових сховищ та пошукових індексів;
 опис застосованих моделей штучного інтелекту, їх призначення, обмежень та умов використання;

інструкцію з розгортання, первинного налаштування, оновлення, резервного копіювання, відновлення та виведення Платформи з експлуатації;

керівництво адміністратора;
 керівництво Користувача;
 опис реалізованих засобів автентифікації, розмежування доступу, журналювання, моніторингу та інших заходів захисту;

опис порядку перевірки, затвердження, відхилення, повернення на уточнення та повторного опрацювання результатів, сформованих Платформою;

методичні рекомендації щодо застосування Платформи у процесах автоматизованого дослідження та технічного аналізу шкідливого програмного забезпечення;

перелік відомих обмежень, залежностей і вимог до супроводу Платформи;
 документацію прикладного програмного інтерфейсу (API), що містить опис методів, форматів запитів і відповідей, моделей даних, механізмів автентифікації та авторизації, кодів помилок, обмежень використання, прикладів взаємодії, інтеграційних механізмів і взаємодії з MSCP-серверами;

6) дослідний зразок програмної платформи локального розгортання із застосуванням технологій штучного інтелекту для підтримки процесів автоматизованого дослідження та технічного аналізу шкідливого програмного забезпечення, придатний до розгортання і дослідної експлуатації в інфраструктурі органу, яким було заявлено зазначену пріоритетну тематику та сформовано відповідне вихідне Технічне завдання;

7) комплект випробувальної документації та матеріали випробувань має включати:
 програму та методику випробувань;
 опис випробувального середовища, конфігурації обладнання і програмного забезпечення;
 опис тестових наборів даних і контрольних зразків;
 тестові сценарії та очікувані результати;
 протоколи функціональних випробувань;
 протоколи інтеграційних випробувань із Ghidra, IDA Pro, x64dbg, прикладними програмними інтерфейсами та MSCP-серверами;
 протоколи перевірки встановлення, оновлення, резервного копіювання та відновлення;
 протоколи випробувань продуктивності, навантажувальної спроможності та стійкості під навантаженням;

протоколи перевірки ізоляції середовища дослідження, обмеження мережевої взаємодії та запобігання неконтрольованому виконанню або поширенню досліджуваних зразків;

протоколи перевірки механізмів автентифікації, розмежування доступу, журналювання, ізоляції даних та інших реалізованих заходів захисту;

результати перевірки стійкості Платформи до некоректних, неповних або надмірних вхідних даних;

результати оцінювання якості роботи модулів штучного інтелекту за визначеними показниками, зокрема методику, показники, контрольні набори даних і граничні значення, за якими оцінюється якість результатів модулів штучного інтелекту;

підсумковий звіт про результати випробувань із висновком щодо відповідності дослідного зразка вимогам цього технічного завдання;

матеріали демонстрації функціональних можливостей Платформи в локальному ізолюваному випробувальному середовищі, що забезпечує функціонування передбачених цим технічним завданням компонентів і проведення встановлених видів випробувань.

5.2. Основні складові частини виготовлених дослідних зразків чи іншої основної виготовленої науково-технічної продукції (за наявності):

Назва складової частини	Необхідна кількість, од.
Програмне забезпечення у складі: підсистема інтеграції з інструментами автоматизованого дослідження та отримання даних про об'єкти дослідження; підсистема попереднього профілювання зразків; підсистема семантичного аналізу програмного коду; підсистема виявлення поведінкових характеристик і технік протидії аналізу; підсистема пошуку схожості та класифікації зразків; підсистема формування захисних артефактів; підсистема формування технічних і аналітичних звітів; підсистема накопичення, пошуку та повторного використання результатів попередніх досліджень; підсистема керування процесом аналізу, перевірки та простежуваності результатів; підсистема взаємодії з Користувачем; підсистема адміністрування, захисту, журналювання та моніторингу.	1 од.
Програмна документація	1 од.
Формуляр	1 од.
Експлуатаційна документація	1 од.
Науково-технічний звіт за формою, визначеною Замовником (обов'язково для всіх тематик)	1 од.

5.3. Перелік додаткових практичних методик, положень, інформаційно-аналітичних матеріалів, рекомендацій, пропозицій до органів влади та інших документів, що можуть бути передані потенційним замовникам для використання, зокрема, на договірних умовах. (заповнюється учасником Конкурсу)

6. Календарний план виконання Розробки (заповнюється учасником Конкурсу)* Строк виконання Розробки - 12 міс.

№ етапу	Етапи виконання робіт, у тому числі етапи робіт співвиконавця	Строк виконання (початок - закінчення), місяць, рік	Науково-технічна продукція та інші матеріали, що підлягають здачі замовнику, у тому числі назва продукції співвиконавця	Вартість робіт за етапами, у тому числі обсяг робіт співвиконавця, тис. грн
---------	---	---	---	---

1	(у тому числі співвиконавець: (найменування співвиконавця та назва її етапу робіт)		(у тому числі співвиконавець: (найменування співвиконавця, назва продукції)	
Всього 1 етап				
2	(у тому числі співвиконавець: (найменування співвиконавця та назва її етапу робіт)		(у тому числі співвиконавець: (найменування співвиконавця, назва продукції)	
Всього 2 етап				
Всього				

** Примітка: Якщо виконання Розробки заплановано на один рік, календарний план та кошторис складаються тільки в його календарних межах. Для Розробки технічного спрямування рекомендуємо при визначенні завдань етапів виконання робіт керуватись ДСТУ 3973-2000 «Система розроблення та поставлення продукції на виробництво. Правила виконання науково-дослідних робіт. Загальні положення» та ДСТУ 3974-2000 «Система розроблення та поставлення продукції на виробництво. Правила виконання дослідно-конструкторських робіт».*

7. Очікуване впровадження та спосіб реалізації результатів Розробки

7.1. Зазначається інформація про вагомість отриманої продукції для України, можливі ринки її збуту; очікувані переваги науково-технічної продукції перед існуючими українськими та/або зарубіжними аналогами; наявні виробничі потужності щодо можливого запуску дослідного/серійного виробництва науково-технічної продукції.
(доповнюється учасником Конкурсу)

Розроблена Платформа матиме вагоме значення для України як засіб підвищення ефективності автоматизованого дослідження та технічного аналізу шкідливого програмного забезпечення в умовах зростання кібернетичних загроз. Її основними перевагами є локальне розгортання в захищеній інфраструктурі органу, яким заявлено зазначену пріоритетну тематику та сформовано відповідне вихідне Технічне завдання, збереження конфіденційності досліджуваних даних, зменшення залежності від зовнішніх хмарних сервісів, інтеграція з поширеними інструментами автоматизованого дослідження, контрольоване застосування технологій штучного інтелекту та можливість адаптації до потреб органу, яким було заявлено зазначену пріоритетну тематику та сформовано відповідне вихідне Технічне завдання.

7.2. Очікуваний ефект для оборони, економіки та/або суспільства, від використання (впровадження) результатів (посилення обороноздатності, створення або збереження робочих місць, збільшення дохідної частини державного бюджету України, суттєве покращення якості життя населення за рахунок поліпшення стану довкілля, медичного обслуговування, транспорту, зв'язку тощо).
(доповнюється учасником Конкурсу)

Впровадження Платформи сприятиме посиленню обороноздатності України та підвищенню спроможності органу, яким заявлено зазначену пріоритетну тематику та сформовано відповідне вихідне Технічне завдання, протидіяти кіберзагрозам. Використання Платформи забезпечить скорочення часу на дослідження шкідливого програмного забезпечення, підвищення повноти й відтворюваності результатів аналізу, стандартизацію роботи аналітиків та прискорення підготовки захисних артефактів, технічних висновків і аналітичних звітів.

Очікуваним результатом є підвищення швидкості виявлення функціональних можливостей шкідливого програмного забезпечення, встановлення його поведінкових характеристик, виявлення технік протидії аналізу та формування засобів виявлення і реагування. Накопичення та повторне використання результатів попередніх досліджень

зменшить обсяг повторюваної ручної роботи, сприятиме збереженню інституційних знань і підвищенню ефективності підготовки фахівців з аналізу шкідливого програмного забезпечення.

Локальне розгортання Платформи забезпечить контроль над досліджуваними зразками та пов'язаними даними, зменшить залежність від зовнішніх сервісів і створить передумови для розвитку в Україні власних технологій та компетентностей у сфері аналізу шкідливого програмного забезпечення і застосування технологій штучного інтелекту в кібербезпеці.

7.3. Визначити та обґрунтувати, яким шляхом та в який спосіб має здійснюватися подальше впровадження, використання очікуваних результатів, на яких підприємствах або організаціях, навести перелік робіт, які необхідно виконати для повної реалізації (впровадження) Розробки (наприклад: передача документації на підприємство для підготовки виробництва; освоєння випуску продукції; створення і апробація дослідного зразка тощо).

(доповнюється учасником Конкурсу)

Подальше впровадження отриманого кінцевого продукту на національному рівні в Україні буде здійснено після передачі документації органу, яким заявлено зазначену пріоритетну тематику та сформовано відповідне вихідне Технічне завдання.
