Додаток 9
до Пріоритетної тематики, за якою буде здійснюватися державне замовлення на науково-технічні (експериментальні) розробки та науково-технічну продукцію у 2026 році

ТЕХНІЧНЕ ЗАВДАННЯ
НА ВИКОНАННЯ НАУКОВО-ТЕХНІЧНОЇ РОБОТИ

1. Назва науково-технічної роботи (далі – НТР)
(заповнюється учасником Конкурсного відбору)

_____

_____

2. Назва пріоритетної тематики державного замовлення на найважливіші науково-технічні (експериментальні) розробки та науково-технічну продукцію для задоволення пріоритетних державних потреб

Розроблення програмного забезпечення для формування, імплементації та контролю технічних заходів забезпечення кібербезпеки в інформаційних системах та мережах.

3. Мета і вихідні дані для виконання НТР

3.1. Мета виконання НТР

Метою є розроблення програмного забезпечення, яке формуватиме безпечні конфігурації інформаційних систем, методів їх автоматизованої імплементації та контролю впровадження, в рамках реагування на кіберінциденти та кібератаки, які дозволять масштабувати безпекові заходи в інформаційно-комунікаційних системах незалежно від рівнів підготовки адміністративного персоналу та забезпечити перевірку виконання цих заходів.

3.2. Проблеми, на вирішення яких має бути спрямована НТР

Широкий спектр програмного забезпечення, що використовується, його поєднання, різноманітність побудови мереж потребує кастомізації необхідних безпечних конфігурацій, автоматизації цих процесів, а також введення механізмів контролю за виконанням. В умовах постійних кібератак з боку хакерських угруповань проти державних органів та об'єктів критичної інфраструктури України існує потреба у впровадженні обов'язкових вимог щодо посилення кібербезпеки та контролю їх виконання, що дозволить знизити можливості з реалізації відомих кібератак та мінімізувати ландшафт кіберзагроз в рамках загальнодержавного механізму реагування.

3.3. Вихідні дані для розроблення науково-технічної продукції

Закон України «Про основні засади забезпечення кібербезпеки України».

Постанова Кабінету Міністрів України від 29 березня 2006 р. № 373 «Про затвердження Правил забезпечення захисту інформації в інформаційних, електронних комунікаційних та інформаційно-комунікаційних системах».

Інформація, яка є необхідною для виконання НТР, зокрема яка є відсутньою у відкритому доступі буде надана Службою безпеки України Виконавцю Розробки за запитом через Замовника в установленому порядку.

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

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

У результаті виконання НТР необхідно розробити програмне забезпечення для формування безпечних конфігурацій інформаційних систем, методів їх автоматизованої імплементації та контролю впровадження, відповідно до виявлених, в рамках реагування на кіберінциденти та кібератаки, технік, тактик та процедур, що використовуються хакерськими угрупованнями.

4.2. Відповідність рівню технологічної готовності (Technology Readiness Levels), який пропонується досягнути в НТР у порівнянні з необхідним

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

Для досягнення зазначеного TRL Виконавцю Розробки буде надано допомогу з боку державного органу, яким було заявлено зазначену пріоритетну тематику та сформовано відповідне вихідне Технічне завдання, у проведенні наступних робіт: тестуванні програмного продукту в робочому середовищі (зокрема, на базі серверних потужностей цього органу), наданні необхідних дозволів, підписанні протоколів випробувань / тестування, наданні зауважень / пропозицій щодо удосконалення / корегування роботи тощо розробленого в рамках цієї НТР програмного продукту тощо.

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

TRL, який необхідний згідно вимог	**TRL, який пропонується**
TRL7	*(заповнюється учасником Конкурсного відбору)*

*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 НТР
технічні (тактико-технічні)	Інформаційне наповнення (далі - ПЗ)			

	має здійснюватися з урахуванням існуючих державних вимог та світових практик Архітектура ПЗ “сервер + агент”: сервер (Linux) з базою даних профілів; клієнт-агент, що виконує аудит, імплементацію та формує звіт. Можливо два варіанти реалізації клієнта: *Варіант А* — єдиний кросплатформенний агент; *Варіант Б* — окремі агенти (Windows/Linux/MacOS). Профілі безпеки: повинно бути забезпечено можливість створення, редагування та видалення профілів і правил, забезпечено контроль їх версій. Профілі повинні бути захищеними цифровим підписом та розповсюджуватися агентам. Агент повинен здійснювати збір параметрів клієнтської операційної системи (Windows 10/11, Windows Server; Linux) та налаштувань інстальованого прикладного програмного забезпечення, здійснювати порівняння з профілем, та надавати відповідний висновок щодо відповідності – pass/warn/fail. **Режим роботи агента** – агент виконує аудит і імплементацію **повністю автономно**, без підключення до сервера. Профілі безпеки завантажуються **вручну** з ізольованого сервера на захищеному носії, а звіти передаються назад тим самим способом.			

експлуатаційні				
фізико-хімічні				
механічні				
якісні				
споживчі				
інші				
Вимоги* *(зазначити необхідні):*				
медичні (клінічні)				
вимоги до надійності / захищеності	ПЗ має забезпечувати доступність до нього з усіх видів операційних систем. Серверна частина має функціонувати на ОС Linux. ПЗ має забезпечувати гнучкість у внесенні даних, їх модифікації та вилученні. Зв'язок клієнта із серверною частиною повинен відбуватися з використанням протоколів TLS 1.3, mTLS, JWT. Повинна здійснюватись перевірка підпису профілів, контроль цілісності клієнта та журналу реєстрації подій.			
вимоги до потужності				
вимоги щодо призначеності				
вимоги щодо ресурсо- та енергозбереження				
вимоги до технологічності	**Інтеграції**: REST API, вебхуки; SIEM/SOAR; експорт у ECS/JSON/CSV. **Контейнеризація сервера:** Docker/Kubernetes			
вимоги безпеки	**Модель доступу:** повинно бути реалізовано RBAC та забезпечено розмежування ролей і аудит доступів; опціонально повинно бути реалізовано можливості 2FA/SSO. **Ізоляція середовищ** – сервер розміщується в ізольованій мережі організації, а агент – на об'єкті перевірки.			

	Взаємодія здійснюється лише через обмін файлами профілів і звітів.			
конструктивні				
вимоги щодо ергономіки та технічної естетики				
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 споживчі (експлуатаційні) характеристики				
інші				

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

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

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

1. Прототип програмного забезпечення ПЗ успішно продемонстровано у робочому середовищі, до складу якого входить: програмна частина, що складається з базового програмного середовища (операційна система), прикладного програмного забезпечення.

2. Програмне забезпечення у складі програмних кодів модулів, що розробляється;
база даних та файли програмного забезпечення, який розробляється;
інструкція з розгортання ПЗ;
інструкція із використання та обслуговування ПЗ;
дозволи на використання бібліотек, компонентів, програмних продуктів у складі розробленого програмного забезпечення.

3. Програмна документація на ПЗ, що включає:
технічне завдання на створене ПЗ;
програму та методику випробувань;

пояснювальну записку з описом функціональних можливостей, інформаційного забезпечення, архітектури, програмного коду, інструкцій щодо формування та підтримки бази даних, опис технологічного процесу обробки та оновлення даних тощо;

інструкцію з розгортання та налаштування ПЗ;

настанову користувача / інструкцію користувача.

4. Програми та методики тестувань розробленого програмного забезпечення.

5. Протоколи тестувань програмного забезпечення.

6. Експертний висновок за результатами державної експертизи у сфері технічного та/або криптографічного захисту інформації або документ про відповідність, виданий органом з оцінки відповідності, який акредитовано національним органом України з акредитації.

7. Навчальні матеріали для роботи з ПЗ.

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 відповідних модулів	1 од.
Програмна документація	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 Конкурсного відбору)*

6. Календарний план виконання НТР

*(заповнюється учасником Конкурсного відбору)**

Строк виконання НТР – 12 місяців.

№ 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 організації - співвиконавця та назва її етапу робіт)		(у тому числі співвиконавець: (найменування організації-співвиконавця, назва продукції)	
			Всього 1 етап	
2	(у тому числі співвиконавець: (найменування організації - співвиконавця та назва її етапу робіт)		(у тому числі співвиконавець: (найменування організації-співвиконавця, назва продукції)	
			Всього 2 етап	
			Всього	

** **Примітка:** Якщо виконання НТР заплановано на один рік, календарний план та кошторис складаються тільки в його календарних межах. Для НТР 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 НТР

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 Конкурсного відбору)

Розроблене програмне забезпечення для формування безпечних конфігурацій інформаційних систем, методів їх автоматизованої імплементації та контролю впровадження дозволить забезпечити автоматизований підхід до реалізації заходів реагування на кіберінциденти та кібератаки відповідно до виявлених технік, тактик та процедур, що використовуються хакерськими угрупованнями. Розроблене програмне забезпечення дозволить в цілому зменшити час на впровадження безпечних конфігурації, перевірку їх налаштувань, що в свою чергу дозволить підвищити рівень кіберстійкості інформаційно-комунікаційних систем.

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 Конкурсного відбору)

Отриманий продукт (програмне забезпечення) сприятиме вирішенню актуальної проблеми з підвищення стійкості до кіберзагроз (hardening), зменшення їх ландшафту, автоматизує процес імплементації технічних заходів реагування та забезпечить скорочення часу на їх реалізацію.

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) НТР (наприклад: передача документації на підприємство для підготовки виробництва; освоєння випуску продукції; створення і апробація дослідного зразка тощо).
(доповнюється учасником Конкурсного відбору)

Подальше впровадження отриманого кінцевого продукту на національному рівні в Україні здійснюватиметься у практичній площині шляхом використання програмного забезпечення в рамках реагування на кібератаки та кіберінциденти щодо органів державної влади та об'єктів критичної інфраструктури.