

Додаток 5
до Пріоритетної тематики, за якою
здійснюватиметься державне замовлення
на найважливіші науково-технічні
(експериментальні) розробки та науково-
технічну продукцію у 2027–2028 роках
(пункт 5)

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 інформаційно-аналітичної системи автоматизованої оцінки та прийняття рішень щодо ступеня небезпечності мережевих ресурсів.

3. Мета і вихідні дані для виконання Розробки

3.1. Мета виконання Розробки

Метою є розроблення автоматизованої інформаційно-аналітичної системи оцінки ступеня небезпечності мережевих ресурсів, яка дозволить автоматизувати процес розрахунку ризику дотичності до кримінальної протиправності (за видами злочинів) мережевого ресурсу та/або його елементів з метою пріоритетного реагування на кримінальні правопорушення, які вчиняються з використанням кіберпростору, у тому числі в межах протидії військовій агресії.

3.2. Проблеми, на вирішення яких має бути спрямована Розробка

Збільшення суспільної активності в кіберсфері спричинило підвищення інтересу правопорушників до використання кіберпростору з протиправною метою. З початком російської широкомасштабної агресії збільшилася кількість інтернет-ресурсів, які використовуються для шахрайських дій, торгівлі зброєю, цінностями, викраденими на території бойових дій тощо. Окремо виділяються ресурси, що містять ознаки вчинення воєнних злочинів та підтримки збройної агресії проти України. Пропонований програмний продукт націлений на автоматизовану ідентифікацію інтернет-ресурсів, які містять ознаки вчинення кримінальних правопорушень, з їх розподілом за видами злочинів та оцінкою ступеня небезпеки. Вказані відомості можуть бути використані для оперативного реагування на криміногенні осередки та створення умов функціонування безпечного національного кіберпростору.

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

Вихідними даними є:

індикаторні системи оцінки ризиків SOCTA (ЄС) та Sleipnir (Канада);

ДСТУ 3973-2000 «Система розроблення та поставлення продукції на виробництво. Правила виконання науково-дослідних робіт. Загальні положення»;

ДСТУ 3974-2000 «Система розроблення та поставлення продукції на виробництво. Правила виконання дослідно-конструкторських робіт»;

ДСТУ 7363:2013 «Метрологія. Програмне забезпечення засобів вимірювальної техніки. Загальні технічні вимоги»;

ДСТУ 3321:2003 «Система конструкторської документації. Терміни та визначення основних понять»;

Кримінальний кодекс України;

Закон України від 21.06.2018 № 2469-VIII «Про національну безпеку України»;

Закон України від 30.06.1993 № 3341-XII «Про організаційно-правові основи боротьби з організованою злочинністю»;

Стратегія боротьби з організованою злочинністю, схвалена розпорядженням Кабінету Міністрів України від 16.09.2020 № 1126-р;

постанова Кабінету Міністрів України від 26.01.2022 № 59 «Деякі питання запровадження в діяльність центральних органів виконавчої влади системи оцінки SOCTA Україна»;

постанова Кабінету Міністрів України від 22 травня 2019 р. № 507 «Про затвердження Порядку проведення огляду громадської безпеки та цивільного захисту Міністерством внутрішніх справ»;

Методика оцінювання загроз серйозної та/або організованої злочинності в Україні (SOCTA Україна), схвалена Міжвідомчою робочою групою з координації запровадження в діяльність центральних органів виконавчої влади системи оцінки SOCTA Україна протокол № 6 від 31.07.2024;

European Union Serious and Organised Crime Threat Assessment (EU SOCTA) 2025 – Revised methodology, 14642/23 REV 2, 21 November 2023. URL: <https://data.consilium.europa.eu/doc/document/ST-14642-2023-REV-2/en/pdf>;

Оцінка загроз серйозної та/або організованої злочинності (звіт про результати оцінювання загроз серйозної та/або організованої злочинності - SOCTA Україна) 2019–2022. URL: <https://mvs.gov.ua/upload/1/8/5/3/8/2/socta.pdf>;

наказ Міністерства внутрішніх справ України від 22.06.2023 № 513 «Про затвердження форм облікових карток «Організована група та злочинна організація», «Сфери злочинної діяльності»;

наказ Міністерства внутрішніх справ України від 08.11.2023 № 902 «Про затвердження Інструкції з формування та ведення інформаційної підсистеми «SOCTA» інформаційно-комунікаційної системи «Інформаційний портал Національної поліції України»;

наказ Міністерства внутрішніх справ України від 26.12.2023 № 22375/14 «Про затвердження Методичних рекомендацій з визначення (оцінювання) стану безпечного середовища в Україні».

Інформація, яка є необхідною для виконання Розробки, але є відсутньою у відкритому доступі, буде надана Виконавцю Розробки 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 розроблено автоматизовану інформаційно-аналітичну систему оцінки ступеня небезпечності мережевих ресурсів (далі - Система), яка призначена для автоматизації процесів збору, обробки та аналізу даних з відкритих джерел (OSINT) з метою виявлення, класифікації та пріоритизації загроз у кіберпросторі.

Функціональне призначення Системи:

ідентифікація підозрілих інтернет-ресурсів за ключовими ідентифікаторами;

розрахунок «індексу небезпечності» ресурсу на основі адаптованих методологій SOCTA та Sleipnir;

формування матриць загроз (ранжування ресурсів за рівнем ризику) та побудова графів зв'язків між розрізненими елементами інфраструктури зловмисників для виявлення злочинних мереж.

Структура Системи повинна включати наступні підсистеми:

інтерфейс користувача у вигляді єдиного вікна, що об'єднує доступ до інших підсистем в залежності від прав доступу, налаштування параметрів роботи та сповіщень;

модуль збору даних, що включає автоматизовані механізми моніторингу ресурсів та отримання необхідних даних про них;

модуль первинної обробки даних, що включає інструменти структурування неструктурованих даних у формат бази даних для подальшої обробки (парсинг);

модуль аналізу даних з інтегрованими інструментами на базі штучного інтелекту для семантичного аналізу текстів та розпізнавання об'єктів на зображеннях з метою розрахунку ризиків за векторами, які визначаються видами кримінальних правопорушень;

модуль звітів, що включає панелі індикаторів, зведені панелі (дашборди) для виведення зведених результатів розрахунку рівня загроз;

модуль систематизації та зберігання даних, що включає інструменти структурування даних про об'єкти дослідження для зручної роботи з ними та пошуку необхідних даних;

модуль адміністрування.

Інтерфейс користувача має дозволяти налаштовувати: критерії небезпечності ресурсів, області моніторингу мережі (за доменами, географією, назвою, описом тощо).

Алгоритм взаємодії структурних елементів / складових Системи:

Модуль збору даних здійснює моніторинг ресурсів за визначеними користувачем критеріями та отримує необхідні для розрахунку «індексу небезпечності» дані про них та передає їх модулю первинної обробки даних. Далі здійснюється розбір даних на окремі частини, які можуть зберігатися в базі даних (текст, зображення), та запис їх у виді структури, яка дозволить провести ефективний аналіз. Далі в модулі аналізу ці елементарні дані за допомогою моделей штучного інтелекту розпізнаються як такі, що відповідають встановленим критеріям небезпечності. За результатами формується висновок, який відображається у дашборді (панелі індикаторів, зведені панелі) модуля звітів із необхідними позначками та поясненнями по окремих критеріях та взагалі. У разі виявлення ресурсу із високим індексом небезпечності Система сповіщує користувача. Зайшовши в модуль систематизації та зберігання даних можна знайти досьє ресурсів за певними параметрами запиту і працювати із окремими досьє (переглянути збережені дані та результати аналізу, запустити повторний моніторинг). Необхідно розробити механізм виявлення дублікатів даних та належності їх до одного ресурсу (наприклад, за наявності піддоменів основного ресурсу) і можливість об'єднувати досьє з іншими, якщо вони належать до одного ресурсу. Модуль адміністрування служить для налаштування конфігурації, контролю доступу, ведення журналу реєстрації.

За необхідності модулі можна об'єднувати та розширювати їх функціонал.

У разі виникнення зміни умов роботи певного модуля, виявлення можливості та періодичної необхідності налаштування його роботи під нові умови, така можливість повинна бути передбачена.

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):

TRL6 - здійснено випуск дослідного зразка, технологію (розробку) успішно продемонстровано у відповідному (промисловому) 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 випробувань (тестувань), наданні зауважень та/або пропозицій щодо удосконалення та/або корегування роботи програмного продукту, розробленого в рамках цієї Розробки тощо.

Розгорнута на базі серверів потенційного користувача Система повинна відповідати вимогам законодавства України та міжнародним стандартам, зокрема: ISO 1087:2019 Terminology work and terminology science – Vocabulary; ISO 7498-2:1989, Information processing systems – Open Systems Interconnection – Basic Reference Model – Part 2: Security Architecture; ISO/IEC 10746-1:1998, Information technology – Open Distributed Processing – Reference model: Overview – Part 1; ISO/IEC 10746-2:2009, Information technology – Open distributed processing – Reference model: Foundations – Part 2; ISO/IEC 2382:2015, Information technology – Vocabulary; ISO/IEC 2382-4:1999, Information technology – Vocabulary – Part 4: Organization of data; ISO/IEC 6523-1:2023 Information technology – Structure for the identification of organizations and organization parts – Part 1: Identification of organization identification schemes.

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
TRL6	<i>(заповнюється учасником Конкурсу)</i>

*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 (заповнюється учасником Конкурсу)
технічні (тактико-технічні)	Рівень продуктивності – одночасне опрацювання задач	До 100		

експлуатаційні	Функціональна придатність, Зручність використання, Можливість модифікацій, Надійність		ISO/IEC 25010: :2025	
фізико-хімічні				
механічні				
якісні	Швидкість			
споживчі	Точність результатів, верифікованість			
інші				
Вимоги* (зазначити необхідні):				
медичні (клінічні)				
вимоги до надійності / захищеності			ДСТУ ISO/IEC TR 29181-5:2016 (ISO/IEC TR 29181-5:2013, IDT)	
вимоги до потужності	Можливість одночасної обробки до 100 задач			
вимоги щодо призначеності				
вимоги щодо ресурсо- та енергозбереження				
вимоги до технологічності	Переносимість, мобільність, сумісність			
вимоги безпеки				
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	Довгострокова технічна та програмна підтримка й супровід			

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.

За результатами виконання Розробки буде створена науково-технічна продукція та програмна документація відповідно до вимог ДСТУ 3321-2003 та ДСТУ 7363:2013:

Програмне забезпечення готової до розгортання автоматизованої інформаційно-аналітичної системи оцінки ступеня небезпечності мережевих ресурсів, яке розроблено відповідно до вимог п. 4 цього вихідного Технічного завдання та включає:

- повний комплект файлів програмного коду модулів Системи, що розробляється;
- початковий дамп бази даних Системи, яка розробляється (файл .sql, який містить повну структуру та початковий вміст бази даних); службові та конфігураційні файли;
- дозволи на використання бібліотек, компонентів, програмних продуктів у складі розробленого програмного забезпечення.

Технічне завдання, що включає деталізовані положення цього вихідного Технічного завдання, зокрема, щодо опису сфери застосування і призначеності, технічних, техніко-економічних та спеціальних вимог, стадій та термінів розроблення.

Пояснювальна записка, що включає схеми та описи алгоритмів, загальний опис функціонування, обґрунтування прийнятих технічних рішень; опис і характеристики точності реалізованих розрахункових алгоритмів; опис методики ідентифікації; опис методів захисту і реалізованих даних.

Опис програмного забезпечення: відомості про логічну структуру і функціонування; структура бази даних; опис функцій, що виконуються, зокрема й послідовність оброблення даних; опис типовизначальних і конструктивних параметрів, зокрема, перелік та опис індикаторів для кваліфікації мережевих ресурсів, розроблений з урахуванням методології СОСТА Україна; алгоритми розрахунку індексів небезпечності та розрахунку ризиків за векторами, які визначаються видами кримінальних правопорушень.

Текст програмного забезпечення: вихідний код з необхідними коментарями; у разі використання стороннього коду, повинен включати дозволи на використання бібліотек, компонентів, програмних продуктів у складі розробленого програмного забезпечення.

Комплект тестової документації: матеріали випробувань (програма та методика випробувань, протоколи тестування (функціонального, навантажувального, безпекового), що підтверджують відповідність системи Технічному завданню та коректність роботи алгоритмів оцінки).

Настанова системного адміністратора: відомості для розгортання, перевірки, забезпечення функціонування і налаштування на умови конкретного застосування Системи.

Настанова користувача: відомості для експлуатації, зокрема опис інтерфейсів користувача, всіх меню і діалогів; характеристики системних апаратних засобів.

Комплект методичного забезпечення (для користувачів-аналітиків): методики автоматизованої оцінки ступеня небезпечності мережних ресурсів, результати верифікації системи: аналіз точності присвоєння індексів небезпечності на контрольних прикладах, включаючи перелік та опис індикаторів для кваліфікації мережевих ресурсів, розроблений з урахуванням методології СОСТА Україна та базу даних та/або таблиці індикаторів для оцінки мережевих ресурсів за напрямками, математичні моделі розрахунку інтегрального показника небезпечності ресурсу з використанням вагових коефіцієнтів для кожного індикатора.

Програма тренінгів для аналітиків щодо інтерпретації матриць ризиків та використання візуалізації (графів) для прийняття управлінських рішень.

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

Назва складової частини	Необхідна кількість, од.
Програмний код системи, файли конфігурації (сервер)	1
База даних	1
Інструкція з використання та обслуговування системи за ролями	1
Науково-технічний звіт за формою, визначеною Замовником (обов'язково для всіх тематик)	1

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 - 18 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 та назва її етапу робіт)	
Всього 1 етап				
2	(у тому числі співвиконавець: (найменування співвиконавця та назва її етапу робіт)		(у тому числі співвиконавець: (найменування співвиконавця та назва її етапу робіт)	
Всього 2 етап				
3	(у тому числі співвиконавець: (найменування співвиконавця та назва її етапу робіт)		(у тому числі співвиконавець: (найменування співвиконавця та назва її етапу робіт)	
Всього 3 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 наявними українськими та/або зарубіжними аналогами; наявні виробничі потужності щодо можливого запуску дослідного/серійного виробництва науково-технічної продукції.

(доповнюється учасником Конкурсу)

Продукція є критично важливою для забезпечення національної безпеки в умовах гібридної війни, оскільки дозволяє обробляти великі масиви даних, які неможливо проаналізувати вручну. Вона забезпечує перехід від реактивного реагування до моделі Intelligence-Led Policing. На відміну від наявних розрізнених інструментів, запропонована система інтегрує методи кримінального аналізу, OSINT та теорію графів в єдиний цикл, використовуючи міжнародно визнані стандарти, що забезпечує сумісність з європейськими системами обміну даними. Реалізація можлива на базі наявних ІТ-підрозділів правоохоронних органів або спеціалізованих науково-дослідних установ Міністерства внутрішніх справ України.

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)

Посилення спроможностей у протидії інформаційним операціям ворога (виявлення «ботоферм», пропагандистських ресурсів) та документуванні воєнних злочинів з використанням OSINT.

Підвищення рівня захищеності громадян від злочинів у кіберсфері шляхом оперативного блокування небезпечних ресурсів, що мають високий індекс небезпечності.

Оптимізація використання людських та фінансових ресурсів правоохоронних органів за рахунок автоматизації рутинних процесів збору даних та фокусування зусиль лише на пріоритетних загрозах.

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)

Впровадження Системи планується здійснювати через департаменти інформаційно-аналітичної підтримки, кіберполіції, кримінального аналізу Національної поліції України, ситуаційні центри Міністерства внутрішніх справ України.

Після інсталяції програмного забезпечення на серверах потенційного користувача, а саме департаментів інформаційно-аналітичної підтримки, кіберполіції, кримінального аналізу Національної поліції України, ситуаційних центрів Міністерства внутрішніх справ України, та передачі технічної документації, планується проведення тренінгів для аналітиків щодо інтерпретації матриць ризиків та використання візуалізації (графів) для прийняття управлінських рішень.
