

Додаток 12
до Пріоритетної тематики, за якою
здійснюватиметься державне замовлення
на найважливіші науково-технічні
(експериментальні) розробки та науково-
технічну продукцію у 2027–2028 роках
(пункт 12)

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 засобу криптографічного захисту інформації різного ступеня обмеження доступу під час зберігання (захист інформації у стані спокою) в складі інформаційно-комунікаційних систем.

3. Мета і вихідні дані для виконання Розробки.

3.1. Мета виконання Розробки

Метою Розробки є розроблення засобу криптографічного захисту інформації (далі – КЗІ) в стані спокою (далі – засіб КЗІ-СС), який призначений для забезпечення конфіденційності, цілісності та автентичності даних в стані спокою в складі інформаційно-комунікаційних систем (далі – ІКС) різного функціонального призначення.

3.2. Проблеми, на вирішення яких має бути спрямована Розробка

Відповідно до статті 8 Закону України «Про захист інформації в інформаційно-комунікаційних системах», умовами оброблення інформації різного ступеня обмеження доступу в системах є, зокрема, авторизація з безпеки таких ІКС, яка, відповідно до положень Порядку авторизації з безпеки інформаційних, електронних комунікаційних, інформаційно-комунікаційних, технологічних систем, затвердженого постановою Кабінету Міністрів України від 18.06.2025 № 712, можлива лише за умов реалізації в ІКС цільового профілю безпеки, який створено на підставі базового профілю безпеки, визначеного та затвердженого Адміністрацією Держспецзв'язку.

Базовим профілем безпеки системи, де обробляється відкрита або конфіденційна інформація, затвердженим наказом Адміністрації Держспецзв'язку від 30.06.2025 № 409, базовим профілем безпеки системи, де обробляється службова інформація, затвердженим наказом Адміністрації Держспецзв'язку від 02.07.2025 № 419, базовим профілем безпеки системи, де обробляється таємна інформація, затвердженим наказом Адміністрації Держспецзв'язку, та базовим профілем безпеки системи, де обробляється цілком таємна інформація, затвердженим наказом Адміністрації Держспецзв'язку, передбачений захід захисту SC-28(1) відповідно до НД ТЗІ 3.6-006-24, а саме реалізація механізмів криптографічного захисту для запобігання несанкціонованому розкриттю інформації під час зберігання (захист інформації у стані спокою).

На теперішній час на ринку України відсутні засоби КЗІ-СС, які оцінені відповідно до законодавства у сфері захисту інформації, та дозволені для криптографічного захисту інформації в стані спокою.

Розробка спрямована на розроблення засобів КЗІ-СС для ІКС, в яких обробляється інформація різного ступеня обмеження доступу (крім інформації, що становить державну таємницю).

3.3. Вихідні дані для розроблення науково-технічної продукції

Розроблена науково-технічна продукція повинна забезпечити відповідність вимогам для засобів КЗІ, передбаченим національними нормативними документами у сфері криптографічного захисту інформації, зокрема:

Технічним регламентом засобів криптографічного захисту інформації, затвердженим постановою Кабінету Міністрів України від 21 жовтня 2020 р. № 991;

переліком стандартів та технічних специфікацій, дозволених для реалізації в засобах криптографічного захисту інформації, затвердженим наказом Адміністрації Держспецзв'язку від 27.10.2020 № 687, зареєстрований в Міністерстві юстиції України 21.12.2020 за № 272/35555;

Положенням про порядок розроблення, виробництва та експлуатації засобів криптографічного захисту інформації, затвердженим наказом Адміністрації Держспецзв'язку від 20.07.2007 № 141, зареєстрованим в Міністерстві юстиції України 30.07.2007 за № 862/14129;

Положенням про державну експертизу в сфері криптографічного захисту інформації, затвердженим наказом Адміністрації Держспецзв'язку від 23.06.2008 № 100, зареєстрованим в Міністерстві юстиції України 16.07.2008 за № 651/15342.

Інформація, яка є необхідною для виконання Розробки, але є відсутньою у відкритому доступі, надається Виконавцю 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

Під час виконання Розробки має бути розроблена програмна та технічна документація на КЗІ-СС та виготовлено зразки засобів КЗІ-СС.

Програмна та технічна документація на засоби КЗІ-СС повинна бути достатньою для організації його серійного виробництва та проведення державної експертизи в сфері криптографічного захисту інформації.

Засіб КЗІ-СС повинен відповідати вимогам щодо стійкості до зовнішніх впливів, ступеня захищеності та живучості.

Засіб КЗІ-СС повинен:

забезпечувати конфіденційність даних, що зберігаються на серверах, робочих станціях, мобільних пристроях, знімних носіях, у базах даних та файлових сховищах;

унеможливлювати несанкціонований доступ до даних у разі компрометації операційної системи, викрадення обладнання, несанкціонованого доступу до дисків або резервних копій, виконання нормативних вимог щодо криптографічного захисту даних у стані спокою.

Засіб КЗІ-СС може бути реалізований як система повнодискового шифрування (Full Disk Encryption), система шифрування на рівні файлів/каталогів, шифрування томів і контейнерів, криптографічний захист баз даних (Transparent Data Encryption), для зберігання ключів шифрування опціонально можливе використання програмно-апаратних токенів та/або модулів (HSM/криптомодулі).

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):

TRL5 – технологію (розробку) перевірено у відповідному (промисловому) середовищі.

Для досягнення зазначеного TRL Виконавцю Розробки буде надано допомогу з боку органу, яким надано пропозиції до пріоритетної тематики та сформовано відповідне вихідне Технічне завдання, у проведенні таких робіт: наданні необхідних дозволів, проведенні тестувань та підписанні відповідних протоколів, наданні зауважень та/або пропозицій щодо удосконалення розробленої науково-технічної продукції, тощо.

Виконавець повинен мати ліцензію на провадження господарської діяльності з надання послуг у галузі криптографічного захисту інформації (крім електронних довірчих послуг та електронної ідентифікації) та технічного захисту інформації за переліком, що визначається Кабінетом Міністрів України.

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
TRL 5	<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:

<i>Характеристики* (зазначити необхідні):</i>				
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)	Криптографічний захист даних на всіх типах носіїв: жорсткі диски		Вимогою замовника	

	(HDD/SSD); мережеві сховища (NAS/SAN); знімні носії (USB, зовнішні диски); віртуальні машини та контейнери.			
	Реалізація типових підходів до шифрування даних у стані спокою: повне шифрування диска (Full-Disk Encryption, FDE); прозоре шифрування даних (Transparent Data Encryption, TDE); шифрування на рівні програми (Application-Layer Encryption, ALE); шифрування на рівні полів (Field-Level Encryption, FLE)		Вимогою замовника	
	Підтримка сучасних квантовостійких несекретних вітчизняних криптографічних алгоритмів	Калина-256/384/512 (за ДСТУ 7624:2014); режими роботи XTS, GCM або CBC з належною обробкою вектора ініціалізації; інші криптоалгоритми, схвалені регулятором	Вимогою замовника	
	Цілісність і автентичність ключів	Безпечне зберігання криптографічних ключів; підтримка HSM/TPM/смарт-карт; захищене управління ключами (Key Management)	Вимогою замовника	
	Механізми автентифікації доступу	Багатофакторна автентифікація; інтеграція з AD/LDAP; контроль доступу на основі ролей	Вимогою замовника	

	Реєстрацію операцій доступу до зашифрованих даних та спроб несанкціонованого доступу, ведення журналу подій		Вимогою замовника	
	Керованість	Централізоване адміністрування; політики шифрування; дистанційне блокування/стирання ключів	Вимогою замовника	
експлуатаційні	Сумісна робота з основними ОС (Windows/Linux/macOS); підтримка віртуалізованих середовищ; відсутність впливу на прикладні системи		Вимогою замовника	
фізико-хімічні			Визначається розробником	
механічні			Визначається розробником	
якісні			Визначається розробником	
споживчі			Визначається розробником	
інші				
Вимоги * (зазначити необхідні):				
медичні (клінічні)	Забезпечити загальноприйняті вимоги		Визначається розробником	
вимоги до надійності/захищеності			Визначається розробником	
вимоги до потужності			Визначається розробником	
вимоги щодо призначеності			Визначається розробником	
			Визначається розробником	
вимоги щодо ресурсо- та енергозбереження			Визначається розробником	
вимоги до технологічності			Визначається розробником	
вимоги безпеки			Визначається розробником	
конструктивні			Визначається розробником	

вимоги щодо ергономіки та технічної естетики			Визначається розробником	
вимоги охорони довкілля, утилізація			Визначається розробником	
спеціальні вимоги (в тому числі на вимогу замовника)			Визначається розробником	
інші				
Необхідні вимоги до умов експлуатації * (у разі необхідності):				
вимоги щодо безпеки під час транспортування та зберігання (забезпечення збереженості) продукції			Визначається розробником	
вимоги щодо експлуатації та ремонту, дотримання яких забезпечує працездатність і безпечність продукції та гарантує спожиткові (експлуатаційні) характеристики	Легкість освоєння персоналом, простота обслуговування дотримання вимог електробезпеки		ДСТУ 7237:2011 ДСанПіН 3.3.6-2002	
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.

У результаті виконання Розробки буде створена і передана Замовнику наступна науково-технічна продукція:

- програмна та технічна документація на засіб КЗІ-СС;
- акт про виготовлення дослідних зразків засобу КЗІ-СС;
- інструкція з використання та обслуговування засобу КЗІ-СС;
- інструкція з налаштування засобу КЗІ-СС;
- настанова/інструкція користувача засобу КЗІ-СС;
- програми та методики випробувань засобу КЗІ-СС;
- протоколи випробувань у відповідному (промисловому) середовищі;
- пояснювальна записка з описом функціональних можливостей засобу КЗІ-СС;
- програмні та/або математичні моделі перевірки функціонування засобу КЗІ-СС.

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

Назва складової частини	Необхідна кількість, од.
Програмна та технічна документація на засіб КЗІ-СС	1

Дослідний зразок засобу КЗІ-СС	3
Формуляр	3
Експлуатаційна документація	3
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 - 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 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 під час визначення 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)

Отримана продукція дозволить забезпечити безпеку державних інформаційних ресурсів у стані спокою.

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)

Наявність на ринку України засобу криптографічного захисту інформації, який забезпечить реалізацію механізмів криптографічного захисту для запобігання несанкціонованому розкриттю інформації різного ступеня обмеження доступу під час зберігання (захист інформації у стані спокою).

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 результатів розробки засобу КЗІ-СС передбачається поетапно, з тісною координацією між науковими установами, підприємствами оборонно-промислового комплексу та силовими структурами України. Основний шлях реалізації — інтеграція розробленої науково-технічної продукції в інформаційно-комунікаційні системи спеціального призначення.
