

Додаток 7
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 інформаційно-комунікаційної системи для обміну науково-технічною інформацією зі ступенем обмеження доступу “Для службового користування”.

3. Мета і вихідні дані для виконання НТР.

3.1. Мета виконання НТР

Метою НТР є розроблення інформаційно-комунікаційної системи для безпечного обміну науково-технічною інформацією зі ступенем обмеження доступу “Для службового користування” (далі - ІКС ДСК) в електронному вигляді.

3.2. Проблеми, на вирішення яких має бути спрямована НТР

В умовах сьогодення під час провадження наукової, науково-технічної діяльності особливої ваги набуває питання вдосконалення та цифровізації процесів обміну науково-технічною інформацією, що містить відомості з грифом обмеження доступу “Для службового користування”.

Така інформація, зокрема, може бути створена та використовуватися під час виконання фундаментальних досліджень, прикладних наукових досліджень і науково-технічних (експериментальних) розробок, а також у процесі взаємодії та обміну інформацією суб’єктів наукової і науково-технічної діяльності та органів державної влади.

НТР спрямована на вирішення проблеми обміну інформацією з грифом обмеження доступу “Для службового користування”.

Розроблення інформаційно-комунікаційної системи для обміну інформацією з грифом обмеження доступу “Для службового користування” дозволить:

- створити безпечну ІКС ДСК обміну даними;
- забезпечити конфіденційність, цілісність, доступність та підзвітність інформації;
- реалізувати систему керування доступом відповідно до ролей і повноважень користувачів;
- організувати аудит дій для контролю режиму оброблення даних;
- підвищити ефективність науково-технічної діяльності через безпечний обмін результатами досліджень.

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

Розроблена науково-технічна продукція повинна відповідати вимогам національних стандартів з питань безпеки, умов застосування, зокрема:

ДСТУ 3396.2-97 Захист інформації. Технічний захист інформації. Терміни та визначення;

НД ТЗІ 1.1-003-99 Термінологія в галузі захисту інформації в комп'ютерних системах від несанкціонованого доступу;

ДСТУ EN ISO/IEC 15408-1:2022 Інформаційні технології. Методи захисту. Критерії оцінювання. Частина 1. Вступ та загальна модель (EN ISO/IEC 15408-1:2020, IDT; ISO/IEC 15408-1:2009, IDT);

ДСТУ ISO/IEC 15408-2:2023 Інформаційні технології. Кібербезпека та захист конфіденційності. Критерії оцінювання безпеки ІТ. Частина 2. Функційні компоненти безпеки (ISO/IEC 15408-2:2022, IDT);

ДСТУ EN ISO/IEC 15408-3:2022 Інформаційні технології. Методи захисту. Критерії оцінювання. Частина 3. Вимоги до гарантії безпеки (EN ISO/IEC 15408-3:2020, IDT; ISO/IEC 15408-3:2008, IDT);

ДСТУ ISO/IEC 27001:2023 (ISO/IEC 27001:2022, IDT) Інформаційна безпека, кібербезпека та захист конфіденційності. Системи керування інформаційною безпекою.

Типова інструкція про порядок ведення обліку, зберігання, використання і знищення документів та інших матеріальних носіїв інформації, що містять службову інформацію, затверджена постановою Кабінету Міністрів України від 19 жовтня 2016 року № 736;

Деякі питання документування управлінської діяльності, затверджені постановою Кабінету Міністрів України від 17 січня 2018 року № 55;

Правила забезпечення захисту інформації в інформаційних, електронних комунікаційних та інформаційно-комунікаційних системах, затверджені постановою Кабінету Міністрів України від 29 березня 2006 р. № 373;

Обов'язкові вимоги до створення (модернізації, модифікації, розвитку), адміністрування та забезпечення функціонування засобу інформатизації, затверджені постановою Кабінету Міністрів України від 21 лютого 2025 року № 205.

Інформація, яка є необхідною для виконання НТР, зокрема яка є відсутньою у відкритому доступі, буде надана центральним органом виконавчої влади, яким було заявлено зазначену пріоритетну тематику та сформовано відповідне вихідне Технічне завдання, Виконавцю НТР за запитом 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

Під час виконання НТР на основі програмного забезпечення Замовника має бути створено, розгорнуто, налаштовано та протестовано мережеву інфраструктуру - ІКС ДСК, функціональним призначенням якої є автоматизація процесів обміну інформацією, в тому числі науково-технічною, та забезпечення режиму обробки інформації з грифом обмеження доступу “Для службового користування”.

Основними складовими ІКС ДСК мають бути:

1. Технічні засоби з мінімально необхідною конфігурацією для функціонування ІКС ДСК: сервер, шлюз захисту, комутатор, робочі місця адміністраторів із засобам криптографічного захисту інформації, робочі місця користувачів, поставлені на розгорнуті в приміщенні Замовника, а також ХХ установ (за необхідності);

2. Комплекс програмного забезпечення (далі – ПЗ) ІКС ДСК Замовника, а саме: загальносистемне програмне забезпечення;

функціональне програмне забезпечення, яке має виконувати наступні функції: розмежування доступу та захисту інформації; обмін електронними документами, що містять службову інформацію, між різними ланками суб'єктів інформаційного обміну (потенційними користувачами) у межах ІКС ДСК;

клієнтське програмне забезпечення, яке має виконувати наступні функції: робота з документами; управління доступом і безпекою; навігація та інтерфейс; інтеграція та взаємодія;

звіти та аналітика; адміністративні функції, в тому числі конструктор для налаштування процедур (конкурси, звітність та інше), який має забезпечити:

- створення адміністратором користувацьких форм для заповнення та подачі інформації;
- конструктор бізнес-процесів для реалізації процесу подачі та опрацювання форм;
- управління експертизою, для забезпечення розподілу експертиз, реалізації процесів передбачених процедурою (робота членів секції, кураторів розробок та інше).

З метою забезпечення належного функціонування створеної та розгорнутої ІКС ДСК (у разі необхідності) мають бути внесені відповідні коригування (зокрема, шляхом внесення змін до конфігурації та топології).

3. Мінімально необхідна конфігурація сервісу електронних довірчих послуг, яка включає програмне забезпечення для роботи з електронними підписами, технічні засоби для їх зберігання та використання (*наприклад, захищені носії*) та організаційні процедури для реєстрації, перевірки та використання сертифікатів в межах ІКС ДСК;

4. Засоби криптографічного захисту службової інформації (типу: “Канал”, “Шифр” тощо).

Створена в результаті виконання НТР продукція у вигляді ІКС ДСК має виконувати наступні функції:

- створення, внесення змін, надання грифу обмеження доступу “Для службового користування”, реєстрації, обліку, доступу, копіювання, розмноження, передачі, отримання, архівного зберігання та стирання документів з грифом обмеження доступу “Для службового користування” тощо;

- обміну електронними документами, які містять службову інформацію, між різними ланками суб’єктів службового діловодства (потенційними користувачами);

- забезпечення захисту інформації;

- застосування кваліфікованого електронного підпису;

- виконання функцій адміністрування, необхідних для експлуатації ІКС ДСК, із забезпеченням максимального розмежування доступу користувачів до інформації з грифом обмеження доступу “Для службового користування” та процесів її обробки;

- забезпечення захисту інформації під час обміну, в тому числі науково-технічною інформацією з підтримкою забезпечення таких властивостей інформації, як конфіденційність, цілісність, доступність, спостережність;

- забезпечення можливостей контролю за процесами обробки інформації з обмеженим доступом в електронному вигляді.

ІКС ДСК призначено для обміну електронними документами, що містять службову інформацію, між типовими суб’єктами електронного діловодства Замовником та іншими потенційними користувачами.

Потенційними користувачами ІКС ДСК можуть бути: міністерства, інші центральні органи виконавчої влади, заклади вищої освіти, наукові установи.

ІКС ДСК має бути розгорнуто, налаштовано та протестовано на базі серверних потужностей Замовника.

Заплановано проведення авторизації з безпеки ІКС ДСК отриманням відповідного авторизаційного листа.

Орієнтовні параметри необхідних серверних потужностей:

- кількість віртуальних процесорних ядер – не менше 12 шт;

- обсяг оперативної пам’яті – не менше 512 Гб;

- обсяг дискового простору – не менше 4 Тб, до 10 Тб;

- кількість IP-адрес – не менше 32 шт;

- безлімітний доступ до мережі не менше 1 Гбіт/с.

Клас автоматизованих систем: 3 клас (багатокомп’ютерний, розрахований на багато користувачів комплекс, об’єднаний в локальну мережу (або кілька мереж) і який має доступ до мережі Інтернет).

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

ІКС ДСК має бути розгорнута, налаштована та протестована на базі серверних потужностей Замовника, процес обробки електронних документів, що містять службову інформацію, має бути продемонстровано представникам Замовника у робочому середовищі (на базі серверних потужностей Замовника).

Для досягнення зазначених TRL виконавець Розробки повинен провести тестування в робочому середовищі з використанням засобів та методів обробки інформації з грифом обмеження доступу “Для службового користування” та забезпечити співпрацю в частині практичної реалізації кінцевої продукції, а саме шляхом її масштабування.

Для досягнення зазначених TRL та вище для виконання Розробки, зокрема в частині організації робіт зі створення та авторизації системи з безпеки, Виконавець повинен мати ліцензію, видану Державною службою спеціального зв'язку та захисту інформації України на провадження господарської діяльності з надання послуг у галузі криптографічного захисту інформації (крім послуг електронного цифрового підпису) та технічного захисту інформації, а також сертифікати, що підтверджують компетенції в сфері інформаційної безпеки відповідно до серії стандартів ISO/IEC 27000.

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
TRL 7	(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*:				
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 (заповнюється учасником Конкурсного відбору)
технічні (тактико-технічні)	Продуктивність системи	Забезпечення одночасної	Вимогою замовника	

		роботи не менше 50 користувачів		
	Рівень доступності системи	Не менше 99%	ISO/IEC 27001:2022 ДСТУ 3396.1-96	
	Підтримка грифу «ДСК»	Повна відповідність вимогам обробки інформації з обмеженим доступом	Вимогою замовника	
фізико-хімічні				
механічні				
Вимоги*				
вимоги щодо призначеності	Забезпечення електронного документообігу службової інформації	Повний цикл обробки (створення, погодження, підпис, реєстрація, архівування)	Вимогою замовника	
	Підтримка обліку доступу та журналювання	100% операцій фіксуються	ISO/IEC 27002:2022	
вимоги до технологічності	Використання стандартних протоколів обміну	HTTPS, TLS 1.3	RFC 5246, ISO 7498-2:1989	
	Сумісність з офісними сервісами	Інтеграція з MS Office, PDF	Вимогою замовника	
вимоги щодо ергономіки та технічної естетики	Інтерфейс користувача	Інтуїтивно зрозумілий, україномовний	ДСТУ ISO 9241-1:2003	
	Доступність	Веб-доступ через браузер	Вимоги WCAG 2.1	
Необхідні вимоги до умов експлуатації*:				
вимоги щодо безпеки під час транспортування та зберігання (забезпечення збереженості) продукції	Конфіденційність	Захист (шифрування) даних під час передачі та зберігання	Вимогою замовника	
	Цілісність	Контроль хешів, цифровий підпис	ISO/IEC 27001:2022	
	Доступність	Безперервна робота, резервування	ISO 22301:2019	
	Режим автоматичного аналізу поточного стану (в реальному стані) та відновлення працездатності	Система моніторингу ІКС ДСК	Вимогою замовника	
вимоги щодо експлуатації та ремонту, дотримання яких забезпечує працездатність і безпечність продукції та гарантує спожиткові (експлуатаційні) характеристики	Гарантійна (технічну) підтримка функціонування створеного НТП не менше 12 місяців з дати підписання Акту приймання-передачі НТП			

	(останній етап) згідно з Календарним планом виконання НТР (безоплатна підтримка, виправлення виявлених помилок, адаптування тощо).			
	Аналіз заходів з кібербезпеки, моніторинг трафіку, активна протидія кіберзагрозам	Контроль шкідливого ПЗ (віруси), сканування портів, аналіз вхідного трафіку	Вимогою замовника	
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.

В результаті виконання НТР буде створена і передана Замовнику наступна науково-технічна продукція:

1. ІКС ДСК для обміну та захисту інформації з обмеженим доступом (остаточна версія – доопрацьована та налагоджена за результатами тестування і успішно продемонстрована в робочому середовищі) у складі: серверу; шлюзу захисту; комутатору; робочих місць адміністраторів із засобам криптографічного захисту інформації, робочі місця користувачів, поставлені на розгортанні в приміщенні Замовника, а також ХХ установ (за необхідності);

2. Технічний проект на ІКС ДСК, у складі:
 пояснювальна записка;
 проектні рішення (архітектура ІКС ДСК, опис компонентів (сервери, мережі, ПЗ), взаємозв'язки, протоколи, модулі, інтеграція з іншими системами);
 схеми (структурні, функціональні, мережеві схеми, топологія, розміщення обладнання, маршрутизація, кабельні плани);
 документи з інформаційної безпеки (політики безпеки, модель загроз, заходи захисту, відповідність НД ТЗІ, ISO/IEC 27001);
 акт обстеження об'єкта (результати аналізу середовища, існуючих систем, інфраструктури, потреб користувачів).

3. Формуляр у складі:
 загальні відомості (повна назва системи, шифр або код проекту, організація-розробник, замовник (відомство, установа), дата складання формуляру, версія або редакція системи);
 технічні характеристики (функціональне призначення ІКС ДСК, склад, архітектура, ПЗ, інтерфейси взаємодії);
 відомості з інформаційної безпеки;
 експлуатаційні відомості (умови функціонування, порядок введення в експлуатацію, обслуговування та супровід);
 додаткові відомості (відповідальні особи, посилання на нормативні документи, примітки та особливості реалізації).

4. Експлуатаційна документація на ІКС ДСК, яка має включати:
 інструкцію (настанову) з розгортання системи (монтажу, налаштування, тестування, введення в експлуатацію, обслуговування, оновлення);

- інструкції (настанови) із використання та обслуговування системи за ролями (системного адміністратора та користувача/ів);
технологічні (функціональні) інструкції.
5. Акт (и) створення ІКС ДСК (у кількості – 1 од.);
6. Програма (и) та методика (и) тестування ІКС ДСК;
7. Протоколи тестування ІКС ДСК в робочому середовищі;
8. Авторизаційний лист з безпеки ІКС ДСК;
9. Акт про введення в експлуатацію ІКС ДСК.

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

Назва складової частини	Необхідна кількість, од.
Технічний проект	1 од.
Формуляр	1 од.
Експлуатаційна документація на ІКС ДСК	1 од.
ІКС ДСК (акт про створення та акт про введення в експлуатацію)	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 – 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)

Ключові переваги:

1) Операційна ефективність: швидкість обробки документів: автоматизація рутинних процесів (реєстрація, погодження, підписання); зменшення помилок: менше людського фактору; централізований доступ: документи доступні з будь-якого місця, за умови належного доступу.

2) Безпека та контроль: контроль версій: збереження історії змін, можливість відстежити, хто і коли редагував документ; розмежування доступу: гнучке налаштування прав доступу відповідно до ролей; шифрування та цифровий підпис: захист службової інформації та юридична значимість документів.

3) Відповідність вітчизняним та міжнародним стандартам: журнал подій: автоматичне логування дій користувачів; інтеграція з системами контролю ризиків: зручне документування заходів безпеки, оцінок ризиків тощо;

4) Економія ресурсів: зменшення витрат на папір, друк і зберігання; менше часу на пошук і обробку документів — більше часу на стратегічні задачі; оптимізація кадрових ресурсів: автоматизація дозволяє перерозподілити навантаження;

5) Покращення взаємодії: швидке погодження між відділами; інтеграція з CRM, ERP, бухгалтерськими системами; можливість зовнішнього обміну документами з контрагентами через захищені канали.

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)

Підвищення рівня інформаційної безпеки в державних органах за рахунок впровадження механізмів обробки службової інформації з грифом “Для службового користування” відповідно до нормативних вимог;

зниження ризиків витоку службової інформації, що має значення для національної безпеки;

підвищення стійкості та захищеності інформаційних процесів у критично важливих структурах, у тому числі під час кризових ситуацій;

оптимізація управлінських процесів у державних установах, що призведе до зменшення витрат часу та ресурсів на обробку документів;

скорочення витрат на паперовий документообіг, логістику та архівне зберігання документів.

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 результатів НТР має передбачати розгортання та інтеграцію ІКС ДСК в інфраструктуру електронного документообігу Замовника. Це забезпечить автоматизацію

процесів обробки, зберігання та передачі документів, а також підвищить рівень захисту інформації та ефективність управлінських рішень.

В подальшому, за умови наявності відповідної нормативно-правової бази, ІКС ДСК може бути масштабована для забезпечення міжвідомчого обміну інформацією між науковими установами, органами виконавчої влади та іншими державними організаціями в межах єдиного інформаційного простору.
