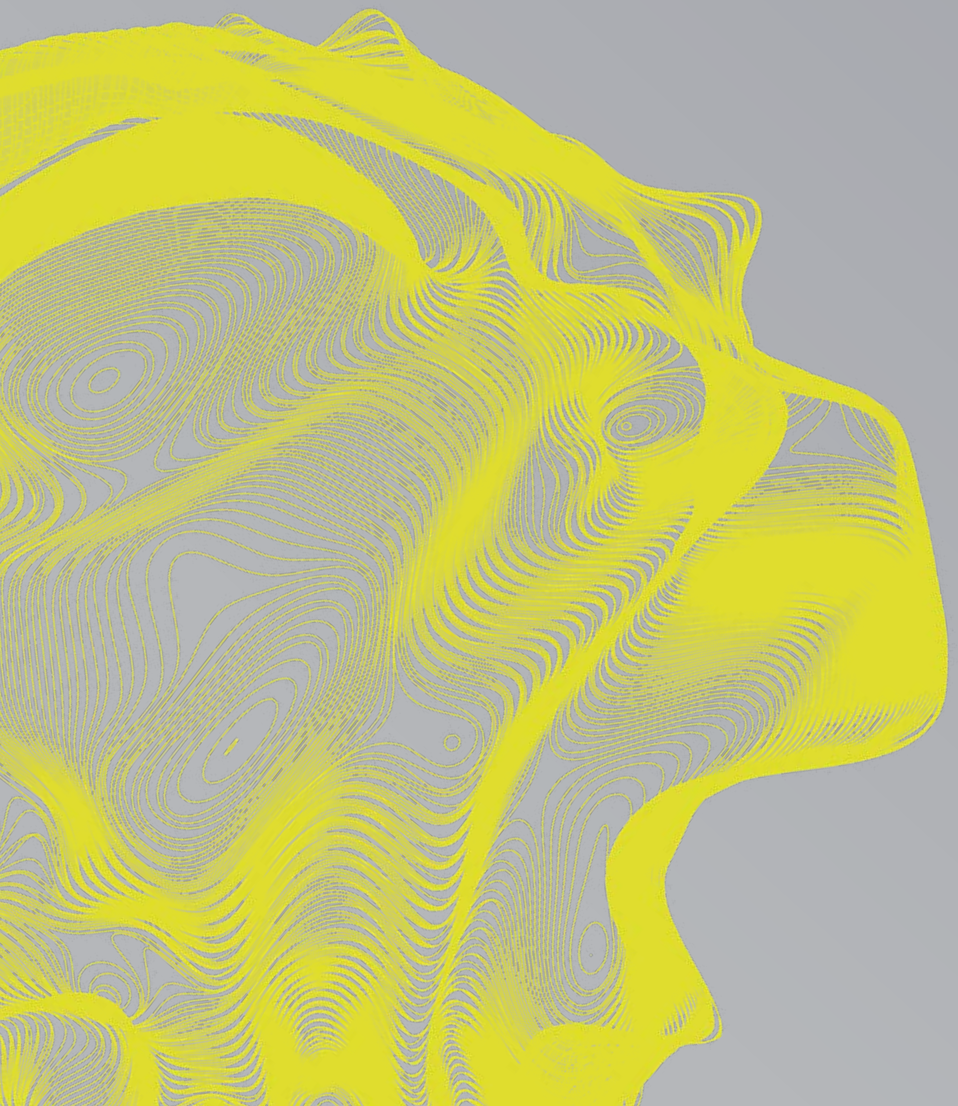
Технології оборонного призначення та інтелектуальна власність:

як захистити розробника, не розкриваючи чутливу інформацію?

IP OFFICE

Український національний офіс
інтелектуальної власності та інновацій

Стратегічна цінність оборонних розробок



У воєнних умовах кожна технологія стає критичним ресурсом. Будь-який витік даних може загрожувати обороноздатності держави й безпеці команди.

Захист інтелектуальної власності в оборонних технологіях – питання національної безпеки.

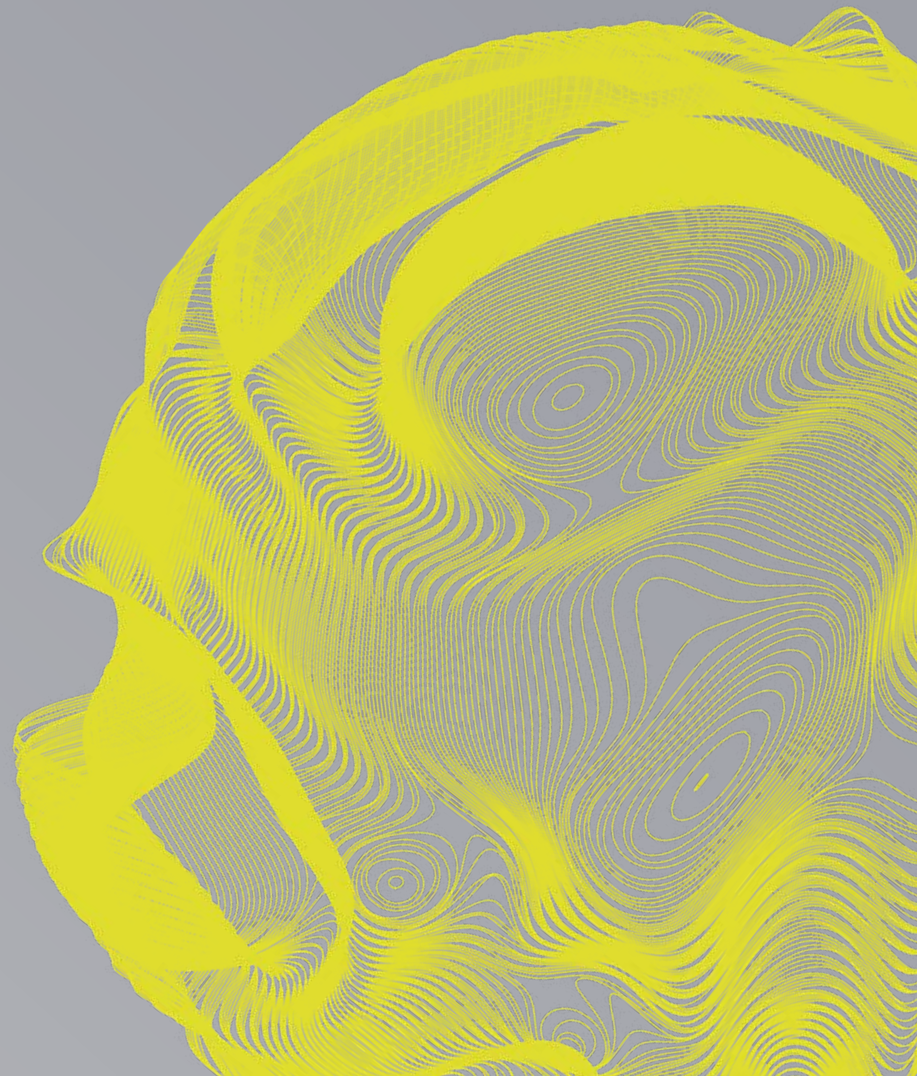
Подвійна потреба в охороні інформації:

1 Дані про винахід:

технічні рішення, алгоритми, елементи,
що можуть містити інформацію,
віднесену до державної або комерційної таємниці.

2 Персональні дані розробників:

прізвище, ім’я, адреса проживання,
контактні дані.

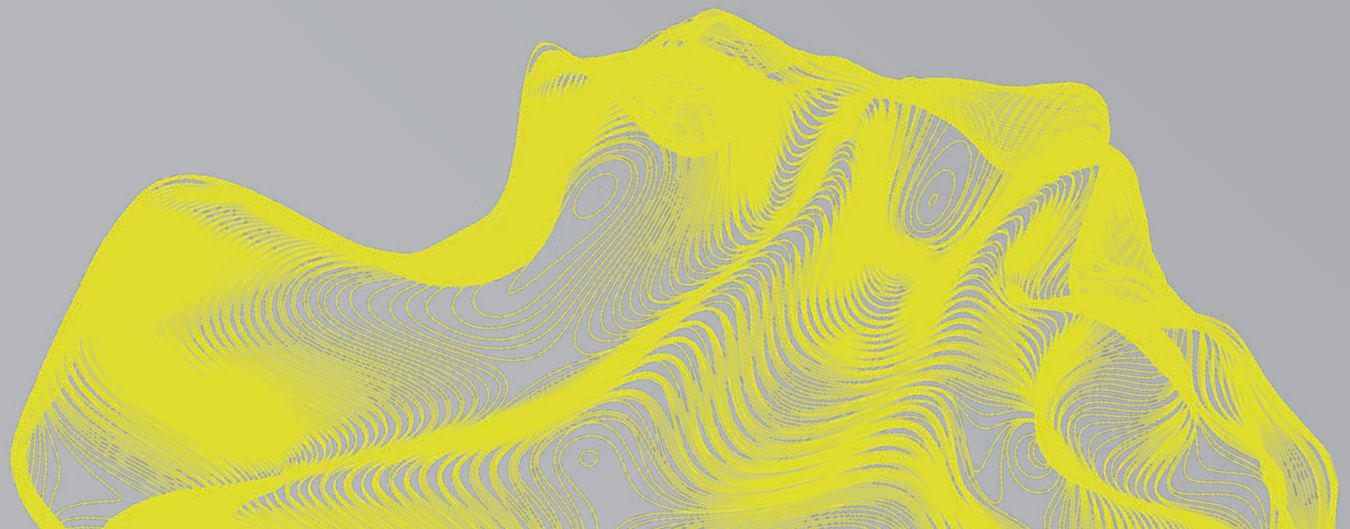


Патент як інструмент юридичного захисту

Реєстрація секретного винаходу або корисної моделі.

Процедура: заявник подає разом із заявкою пропозицію щодо віднесення винаходу або корисної моделі до державної таємниці, після перевірки та ухвалення рішення держава забезпечує заходи для запобігання розголошенню такої інформації.

Схожий механізм діє в США: USPTO та оборонні агентства можуть накладати наказ про секретність, що блокує публікацію оборонних технологій і обмежує їхнє використання, якщо винахід загрожує національній безпеці.



Захист конфіденційної інформації, пов'язаної з технологією

Основні механізми:

- укладення договорів про нерозголошення (NDA) на всіх етапах проєкту: із співробітниками, підрядниками, партнерами та інвесторами;
- **впровадження внутрішніх політик конфіденційності;**
- регламентація порядку доступу до технічної документації;
- **встановлення чітких правил поводження з конфіденційними даними.**

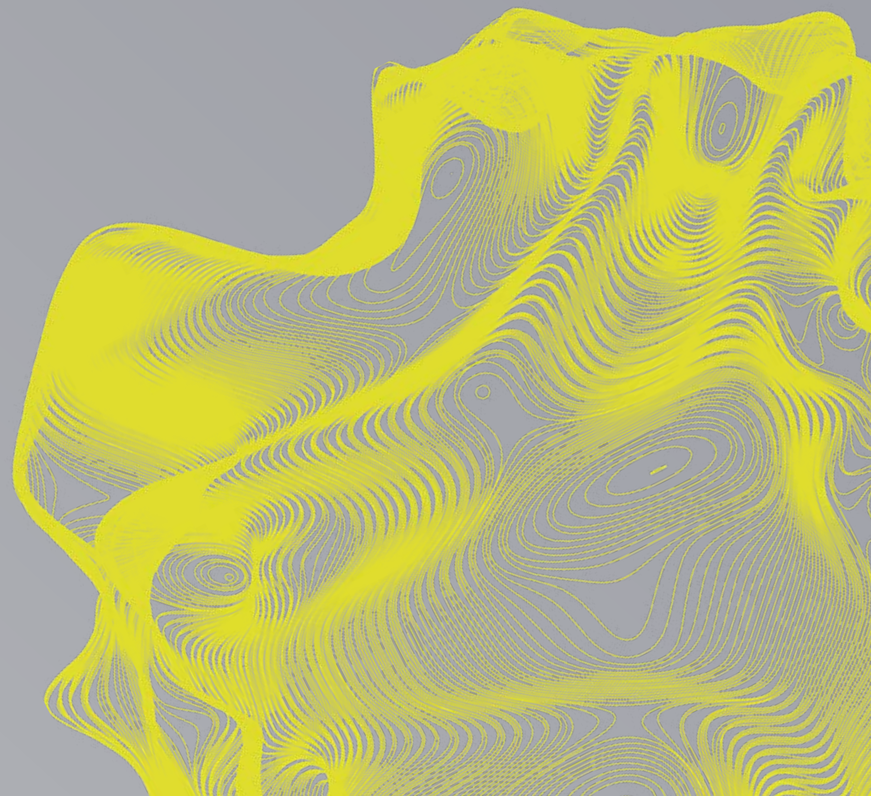
Підхід часткового розкриття даних: безпека та контроль критичної інформації

- Під час патентування розкривати некритичні елементи технології.
- **У ліцензіях та договорах передавати лише обмежений обсяг необхідних даних.**
- На виробництві забезпечувати доступ лише до потрібних для роботи фрагментів технології.
- **Створювати зони обмеженого доступу, де повний обсяг інформації доступний лише визначеним категоріям працівників.**

Комплексний захист інформації = поєднання правових інструментів і організації внутрішніх процесів

Конфіденційність підтримується через внутрішні політики, чіткі процедури та культуру інформаційної безпеки: регулярне навчання персоналу, правила роботи з даними та поводження з обмеженою інформацією.

Цифровий захист включає шифрування файлів і баз даних, контроль доступу, аудит дій та моніторинг операцій для своєчасного реагування на ризики.



IP OFFICE

Український національний офіс
інтелектуальної власності та інновацій

Захист оборонних технологій – ключ до безпеки та стійкості держави

Сайт УКРНОІВІ

+380 (44) 494-05-51

office@nipo.gov.ua

м. Київ, вул. Дмитра Годзенка, 1