ЖИТОМИРСЬКА ПОЛІТЕХНІКА
ДЕРЖАВНИЙ УНІВЕРСИТЕТ

@ZTUEDUUA

ТЕМА 7. ТРАНСФЕРТ НАУКОЄМНИХ ТЕХНОЛОГІЙ ПОДВІЙНОГО ПРИЗНАЧЕННЯ

План

1. **Ліцензування та оцінка наукоємних розробок подвійного призначення**
2. **Форми та моделі трансферту технологій у науковій і освітній діяльності**
3. **Державний експортний контроль технологій подвійного призначення**
4. **Міжнародно-правові договори та режими контролю експорту технологій**
5. **Моніторинг і виявлення порушень у сфері трансферту технологій**
6. **Цифрові інструменти виявлення нелегального експорту технологій**

Розробки подвійного призначення – це технології, наукові знання, матеріали чи програмне забезпечення, які можуть бути використані як у цивільних, наукових, освітніх або економічних цілях, так і для створення або підтримки військових, оборонних чи неконтрольованих технологій.

Приклади:

- наноматеріали, які застосовують у медицині та одночасно в озброєнні;
- штучний інтелект для аналізу даних, що може бути використаний у військовій розвідці;
- роботизовані системи, що мають як цивільні, так і оборонні застосунки;
- біотехнології, що дозволяють створювати вакцини та потенційно біоагенти.

Наукові розробки – це не лише результат інтелектуальної праці, але й потенційний ресурс, який може бути:

- використаний для соціального добробуту (медицина, освіта, екологія),
- або для шкоди (озброєння, контроль населення, кіберконфлікти).

У зв’язку з цим суспільство та держави:

- вводять нормативні обмеження;
- встановлюють процедури оцінки ризиків;
- створюють механізми ліцензування;
- регламентують використання наукових результатів.

Правові основи регулювання у світі та в Україні

Міжнародні загальні підходи

У багатьох країнах і на міжнародному рівні регулювання розробок подвійного призначення здійснюється через:

- режим контролю за експортом технологій;
- переліки товарів та технологій подвійного призначення (Dual-Use Goods Lists);
- міжнародні домовленості (WA, MTCR, Wassenaar Arrangement тощо);
- спеціалізовані агентства, що контролюють експорт, імпорт і використання таких технологій.

Це не лише торговельне питання — це питання безпеки і стабільності.

Український правовий контекст

У національних правових системах, зокрема в Україні, нормативи визначають:

- перелік технологій, робіт і розробок, що можуть бути класифіковані як подвійного призначення;
- процедури отримання дозволів та ліцензій на здійснення робіт;
- вимоги до безпеки та контролю доступу (у т.ч. у наукових установах);
- санкції за порушення правил.

Законодавство щодо контролю за діяльністю у сфері оборонно-промислового комплексу, обігу стратегічних товарів і робіт, а також окремі постанови Кабінету Міністрів України регламентують ці процеси.

Ліцензія – це офіційний документ, що надає право здійснювати певну діяльність, яка без такого дозволу є обмеженою або забороненою.

У випадку технологій подвійного призначення ліцензія:

- гарантує відповідність діяльності вимогам безпеки;
- дозволяє контролювати потоки технологій;
- мінімізує ризики передачі чутливої інформації;
- захищає наукову спільноту від юридичних ризиків.

Ліцензія може вимагатися для:

- розробки технологій, що входять до переліку подвійного призначення;
- передачі технологій, програм або даних;
- участі у контрактах або грантах, пов’язаних із критичними секторами;
- експорту, імпорту, оприлюднення певних результатів.

Наукоємна розробка – це результат науково-дослідної діяльності, який має:

- значний інтелектуальний зміст;
- технологічну складність;
- потенційний економічний або прикладний ефект;
- можливий вплив на безпеку, оборону або інфраструктуру.

Оцінка наукоємної розробки включає:

Визначення потенціалу використання в оборонних цілях або зловмисних сценаріях (алгоритм для аналізу медичних зображень може бути адаптований для автоматичної ідентифікації об’єктів у військових системах);

Оцінка рівня доступності та поширення (якщо розробка є відкритою і може бути легко використана, ризик розповсюдження зростає);

Оцінка чутливих складових (аналіз того, чи містить розробка алгоритми, матеріали, дані або компоненти, які можуть бути використані для створення зброї або засобів тиску);

Міждисциплінарний аналіз (Залучення експертів із права, етики, безпеки, технологій).

Процедура ліцензування

Етап 1. Ідентифікація об’єкта контролю (визначення, чи входитиме розробка до переліку, щодо якого потрібне ліцензування);

Етап 2. Підготовка пакету документів (опис розробки; технічні характеристики; пояснювальна записка; оцінка ризику; юридична інформація про організацію);

Етап 3. Подача заявки до компетентного органу (в Україні – це уповноважені державні органи, що здійснюють контроль за оборонно-промисловою сферою.

Етап 4. Оцінка і експертиза (експертна комісія аналізує ризики, відповідність вимогам, потенційний вплив на безпеку);

Етап 5. Видача або відмова в ліцензії (заявник отримує позитивний документ або негативне рішення з обґрунтуванням).

Трансфер технологій – це процес передачі знань, наукових результатів, технологічних рішень і компетенцій від суб'єкта, що їх створив (університет, НДІ, стартап), до користувача – підприємства, державної установи, соціальної організації або іншого дослідницького кола.

Це **ключовий механізм комерціалізації науки**, перетворення інтелектуальних надбань у продукти, послуги, процеси, які застосовуються у реальному житті.

Усвідомлення трансферту технологій важливо, оскільки саме це дозволяє:

- здійснювати вплив на економіку та суспільство;
- підвищувати життєздатність наукових ідей;
- забезпечувати міждисциплінарну співпрацю;
- будувати кар'єру в академічному, корпоративному та підприємницькому середовищі.

Сутність трансферту технологій: що передається і кому

Передаються:

- Наукові результати – публікації, відкриття, моделі;
- Технологічні рішення – прототипи, алгоритми, методи;
- Інтелектуальна власність – патенти, ноу-хау;
- Компетенції – знання, навички, експертиза.

Отримувачі:

- Промислові підприємства – адаптація технологій для виробництва;
- Малі і середні підприємства (МСП) – інноваційні запускові проєкти;
- Урядові та громадські організації – соціальні інновації, моделі управління;
- Освітні установи – модернізація навчальних програм, методик.

Основні форми трансферту технологій

1. Ліцензування – це надання права користуватися технологією або інтелектуальною власністю за визначених умов.

Механізм:

- Технологія залишається у власності розробника/університету.
- Інший суб’єкт отримує право використовувати її за контрактом.
- Умови: роялті, ексклюзивність/неексклюзивність, термін.

Переваги:

- Захист прав автора;
- Прибутковість для університету;
- Регульованість використання.

2. Продаж прав (assignment) – це повна або часткова передача прав на технологію іншій організації.

Механізм:

- Власник передає майнові права за компенсацію.
- Після цього отримувач має право використовувати технологію без подальших зобов’язань перед автором.

3. Спільні підприємства (joint ventures) і партнерства

Механізм:

- Університет і компанія створюють окрему юридичну особу, яка спільно розвиває й комерціалізує технологію.
- Прибуток і ризики розподіляються між партнерами.

4. Обмін знаннями через партнерські дослідження – це форма, коли університети і компанії працюють разом над спільними проєктами, обмінюючись знаннями, кадрами, даними.

Механізм:

- Компанія інвестує у дослідження;
- Вчені отримують доступ до реальних завдань;
- Технологія створюється спільно.

5. Консультаційні та тренінгові послуги

Університет або наукове підприємство надає:

- експертні консультації;
- навчальні програми;
- адаптовані тренінги для компаній чи організацій.

6. Комерційні стартапи та підприємництво випускників

Студенти, аспіранти або викладачі створюють компанію на основі своєї ідеї.

Механізм:

- Початкові технології можуть бути захищені патентами;
- Стартап отримує ліцензію на їх використання;
- Це дозволяє створювати інноваційні продукти на ринку.

Моделі трансферту технологій

1. Лінійна модель – це традиційна модель, де технологія створюється, потім передається на ринок.

Етапи:

- Наукові дослідження;
- Розробка прототипу;
- Захист інтелектуальної власності;
- Комерціалізація через ліцензування/продаж.

2. Каскадна (еластична) модель – ця модель враховує зворотний зв’язок:

- Комерційні потреби надходять від бізнесу;
- Адаптуються під наукові дослідження;
- Після розробки знову повертаються до бізнесу для впровадження.

Це більш гнучка, сучасна модель, що стимулює інтеграцію науки і практики.

3. Мережеві моделі – трансфер технологій відбувається через мережі взаємодії:

- альянси університетів;
- кластерні об’єднання;
- наукові парки;
- технологічні хаби.

Переваги:

- колективний доступ до ресурсів;
- обмін компетенціями;
- спільна екосистема інновацій.

4. Модель відкритих інновацій

Це стратегія, коли нові ідеї приходять не лише зсередини організації, а й зовні:

- відкриті платформи для співпраці;
- краудсорсинг;
- публічні хакатони;
- відкритий код.

Інституційні механізми трансферту

1. Технопарки і бізнес-інкубатори – це організації, що створюють умови для розвитку інновацій:

- приміщення;
- доступ до обладнання;
- консультації;
- зв’язки з інвесторами.

2. Ліцензійні офіси університетів – університети часто мають спеціальні підрозділи, що:

- оцінюють потенціал розробок;
- шукають стратегічних партнерів;
- укладають ліцензійні угоди;
- забезпечують захист ІВ (інтелектуальної власності).

3. Наукові парки та інноваційні центри – це територіальні об’єднання, що сприяють:

- междисциплінарній співпраці;
- зв’язку науковців та підприємств;
- розвитку стартапів.
- фізичній інтеграції науки і бізнесу.

Значення трансферту технологій

1. Соціально-економічне: створення робочих місць; підвищення продуктивності; диверсифікація економіки; конкурентоспроможність на міжнародному рівні.

2. Академічне: поліпшення навчальних програм; практичний досвід для студентів / аспірантів; залучення фінансування; міждисциплінарні проєкти.

3. Культурне: формування інноваційної культури; розвиток підприємницького мислення; відкритість до змін.

Виклики трансферту технологій

Нормативні перешкоди: складне патентне законодавство; невизначені права інтелектуальної власності; бюрократія при укладанні угод.

Розрив між наукою і бізнесом

- різні мотивації;
- різна культура (довготривалість vs швидкість ринку);
- недовіра до комерційних партнерів.

Нестача фінансування

- розвиток прототипів потребує значних ресурсів;
- ризики для приватних інвесторів.

Етичні та правові аспекти

- справедливий розподіл прибутків;
- дотримання ліцензійних угод;
- невикористання сумнівних технологій;
- прозорість у співпраці;
- повага прав інтелектуальної власності.

Аспірант повинен розуміти, що трансфер технологій – це не лише бізнес, а й етична відповідальність.

Експортний контроль – це система державних заходів, спрямованих на:

- обмеження передачі товарів, технологій та послуг, які можуть мати **військове або подвійне використання**;
- запобігання поширенню озброєнь, технологій, які можуть бути використані для шкоди безпеці;
- дотримання міжнародних зобов’язань;
- захист національних інтересів.

Даний контроль стосується не лише фізичних товарів, а й **технологій, програмного забезпечення, наукових знань та навіть даних**.

У той же час він не є «самоціллю» – він має балансувати між національною безпекою та свободою науки, торгівлі та міжнародної співпраці.

Що таке «технології подвійного призначення»

“Подвійне призначення” – це коли технологія, знання чи продукт може використовуватись як:

✓ у цивільних, мирних цілях (медицина, освіта, енергетика),

✓ так і у військових, оборонних або загрозливих сферах.

Приклади:

- система позиціювання GPS – використовується цивільними, але може бути частиною військових навігаційних систем;
- роботизовані платформи – для виробництва чи роботи в небезпечних умовах, але можуть служити автономними військовими пристроями;
- деякі генетичні інструменти – для діагностики, але мають потенційне застосування у біоозброєнні;
- алгоритми машинного навчання – в науці, але можуть бути адаптовані для розвідки чи кібернетичних атак.

Тобто йдеться про **суть та контекст використання**, а не про саму науку як добру чи погану. Тому контроль цих технологій є складним і потребує балансу.

Навіщо існує державний експортний контроль

Основні цілі:

Національна безпека – не допустити передачу критичних технологій потенційно ворожим країнам або організаціям.

Виконання міжнародних зобов'язань – участь у режимах контролю (наприклад, Wassenaar Arrangement).

Запобігання розповсюдженню озброєнь – біологічних, хімічних, кібернетичних, ракетних тощо.

Контроль за високотехнологічними товарами – наприклад, супершвидкісні комп'ютери або системи шифрування.

Гарантування прозорості міжнародної торгівлі.

Правові основи: міжнародні та національні вимоги

1. Міжнародна складова

Найважливіші міжнародні механізми контролю:

- **Wassenaar Arrangement** – режим контролю за експортом товарів та технологій подвійного призначення.
- **MTCR (Missile Technology Control Regime)** – контроль за технологіями ракетного призначення.
- **NSG (Nuclear Suppliers Group)** – контроль за ядерними матеріалами та технологіями.
- **Australia Group** – контроль над хімічним та біологічним матеріалами.

Ці механізми не є союзними органами ООН, але країни-учасниці добровільно впроваджують їхні переліки до національного законодавства.

2. Національне право

В Україні експортний контроль регулюється:

- законами про режим контролю за обігом товарів і технологій подвійного призначення;
- нормативами про оборонну промисловість;
- постановами про порядок видачі ліцензій;
- спеціальними клубами чи реєстрами (державні списки товарів/технологій під контролем).

Ці документи визначають:

- перелік технологій під контролем;
- вимоги щодо ліцензування;
- порядок подання заявок;
- відповідальність за порушення.

Що саме потрапляє під експортний контроль

1. Товари

Фізичні об’єкти, наприклад:

- мікроелектроніка;
- лазерні системи;
- ракетні компоненти;
- високоточні вимірювальні пристрої.

2. Технології та програмне забезпечення

Це не «коробковий продукт», а знання чи методи, які мають:

- опис алгоритмів;
- методику виробництва;
- ноу-хау.

Приклад:

Програмне забезпечення для управління безпілотними системами може бути контрольованим, навіть якщо сам код не є фізичним товаром.

Як працює експортний контроль на практиці

1. Переліки під контролем

Кожна країна має **список товарів і технологій**, що підлягають контролю. Це документ, де для кожної позиції:

- наводиться опис;
- зазначається код;
- вказуються можливі обмеження.

2. Ліцензування передачі

Підприємство або дослідник, котрий хоче:

- продати;
- передати;
- оприлюднити;
- опублікувати;
- поширювати такі технології іноземним особам чи організаціям, повинен отримати **ліцензію**.

Це може стосуватися:

- прямої передачі технологій;
- спільної роботи з іноземцями;
- академічних публікацій, що описують технічні подробиці;
- участі в міжнародних проектах.

3. Особливості контролю в науковій діяльності

Наука традиційно базується на відкритості:

- публікації;
- обміни студентами;
- міжнародні проєкти;
- відкриті конференції.

Експортний контроль представляє **напруження між відкритістю науки і безпековими вимогами**.

Типові приклади:

- Публікація детального алгоритму для криптографії.
- Опис технології для обробки біомедичних даних, що є частиною озброєння.
- Передача прототипу дослідницького обладнання іноземним партнерам без дозволу.

Тому в науковій сфері контроль стосується не лише товарів, а й:

- статей
- технічних презентацій
- відкритого коду
- описів методів

Як здійснюється процедура контролю

1. Ідентифікація

Науковець або організація визначає, чи може:

- класифіковане як підконтрольне.
- технологія;
- знання;
- програмне забезпечення;
- бути

2. Подача заявки до компетентного органу

Подається:

- опис технологій;
- документи про дослідження;
- пояснення щодо цілей співпраці;
- можливі ризики передачі.

3. Оцінка

Група експертів:

- аналізує потенційний ризик;
- вивчає можливі сценарії використання;
- оцінює відповідність міжнародним та національним вимогам.

4. Рішення

Може бути:

- позитивним – видається ліцензія;
- умовним – тільки за певних гарантій;
- відмовленим.

Зони особливої уваги

1. Біотехнології

Оскільки дані можуть бути використані і для лікування, і для біоагресії.

2. ШІ та алгоритми розпізнавання

Можуть бути адаптовані для військових цілей.

3. Криптографія

Захист даних у цивільних системах можливо співзвучний захисту військових комунікацій.

Вплив на академічну кар’єру і публікації

Експортний контроль може впливати на:

- публікації із детальними технічними розділами;
- участь у міжнародних грантах;
- спільні з іноземцями проєкти;
- відкритий доступ до результатів.

Аспіранти повинні враховувати, що **надмірно детальний технічний опис може потребувати узгодження із компетентними органами**, навіть якщо він публікується у відкритому доступі.

Як захищати свою наукову діяльність і уникати порушень

Своєчасна консультація

Перед:

- публікаціями;
- міжнародною співпрацею;
- передачею коду/даних;
- участю в іноземних проектах;
- варто порадитися з відповідальними особами університету або компетентними контролюючими органами.

Етичні аспекти контролю

Хоча контроль спрямований на захист безпеки, він може створювати:

- перешкоди науковій свободі;
- бар’єри для міжнародної співпраці;
- конфлікти між колективами.

Тому етична позиція аспіранта повинна поєднувати:

- відповідальність;
- критичне мислення;
- розуміння наслідків

Міжнародні стандарти і співпраця

Багато міжнародних організацій вимагають дотримання стандартів експортного контролю:

- для фундаментальної науки;
- для прикладних розробок;
- для спільних досліджень.

Це означає, що академічні установи у різних країнах співпрацюють, узгоджують правила, обмінюються досвідом.

Загальна логіка міжнародного контролю технологій

Міжнародний контроль експорту технологій виник як відповідь на загрозу:

- розповсюдження ядерної, хімічної та біологічної зброї;
- розвитку ракетних систем;
- передачі критичних технологій державам, що можуть використовувати їх у воєнних або терористичних цілях;
- неконтрольованої мілітаризації новітніх наукових досягнень.

Основна ідея полягає не в забороні науки чи торгівлі, а в **регульованому та відповідальному використанні технологій**, які можуть мати подвійне призначення.

Що таке міжнародно-правовий режим контролю

Міжнародний режим контролю – це система:

- договорів,
- угод,
- принципів,
- переліків контрольованих товарів,
- процедур співпраці між державами, які спрямовані на обмеження поширення чутливих технологій.

Важливо розуміти:

Більшість режимів контролю не є класичними договорами з жорсткою санкційною системою. Це механізми координації та взаємних зобов’язань держав.

Ключові міжнародні договори

1. Договір про нерозповсюдження ядерної зброї (NPT)

Мета:

- запобігти поширенню ядерної зброї;
- сприяти мирному використанню атомної енергії;
- стимулювати роззброєння.

Значення:

- встановлює обмеження на передачу ядерних матеріалів і технологій;
- запроваджує систему гарантій МАГАТЕ;
- зобов’язує держави впроваджувати контроль експорту ядерних технологій.

Для аспірантів:

Навіть мирні дослідження в галузі ядерної енергетики підпадають під міжнародний контроль.

2. Конвенція про заборону хімічної зброї (CWC)

Мета:

- повна заборона розробки, виробництва та використання хімічної зброї.

Механізми:

- контроль хімічних речовин;
- інспекції;
- переліки контрольованих сполук.

Це означає, що деякі хімічні дослідження потребують спеціального дозволу на експорт або передачу.

3. Конвенція про заборону біологічної зброї (BWC)

Забороняє:

- розробку,
- накопичення,
- передачу біологічних агентів у воєнних цілях.

Проблема:

- складність перевірки дотримання;
- подвійне використання біотехнологій.

Це створює складний баланс між наукою та безпекою.

4. Договір про торгівлю зброєю (ATT)

Мета:

- встановлення стандартів міжнародної торгівлі озброєннями;
- запобігання незаконному обігу.

Неформальні (координаційні) режими контролю

Ці режими не є договорами ООН, але мають значний вплив.

1. Wassenaar Arrangement

Основна сфера:

- товари та технології подвійного призначення;
- звичайні озброєння.

Особливості:

- країни добровільно погоджують переліки контрольованих товарів;
- встановлюють стандарти прозорості;
- координують експортні обмеження.

Цей режим охоплює:

- кіберінструменти,
- криптографію,
- штучний інтелект,
- мікроелектроніку.

Для аспірантів:

Деякі алгоритми, програмне забезпечення або апаратні розробки можуть входити до переліків цього режиму.

2. Missile Technology Control Regime (MTCR)

Спрямований на:

- контроль ракетних технологій;
- обмеження передачі безпілотних систем;
- регулювання двигунів, матеріалів, навігаційних систем.

3. Nuclear Suppliers Group (NSG)

Контролює:

- ядерні матеріали;
- обладнання;
- технології збагачення урану;
- реакторні компоненти.

4. Australia Group

Спрямований на:

- контроль біологічних і хімічних матеріалів;
- координацію переліків небезпечних агентів.

Механізми реалізації міжнародних режимів

Міжнародні режими працюють через:

- Розробку спільних переліків.
- Імплементацію у національне законодавство.
- Ліцензування експорту.
- Обмін інформацією між державами.
- Санкційні механізми.

Держава повинна:

- включити міжнародні списки до внутрішнього права;
- створити уповноважені органи;
- забезпечити контроль виконання.

Баланс між науковою свободою і безпекою

Міжнародні режими стикаються з проблемою:

- Як не обмежити фундаментальну науку, але водночас запобігти її зловживанню?

Фундаментальні дослідження, як правило, не підлягають жорсткому контролю, але:

- прикладні технології;
- технічна документація;
- інженерні рішення – можуть вимагати ліцензії.

Вплив на університети та аспірантів

Міжнародні режими можуть впливати на:

- міжнародні гранти;
- спільні публікації;
- передачу програмного забезпечення;
- участь у міжнародних проєктах.

Аспірант має враховувати:

- можливі обмеження при співпраці з іноземними партнерами;
- необхідність узгодження передачі технологій;
- відповідальність за порушення режимів.

Нові виклики: цифрова епоха

Сучасні технології ускладнюють контроль:

- передача коду через хмару;
- відкритий доступ до алгоритмів;
- дистанційна співпраця;
- цифрові платформи.

Контроль більше не стосується лише фізичного експорту – він стосується інформаційних потоків.

Геополітичний вимір

Експортний контроль став інструментом:

- технологічної конкуренції;
- санкційної політики;
- обмеження доступу до напівпровідників;
- контролю штучного інтелекту.

Це впливає на:

- глобальні ланцюги постачання;
- міжнародну академічну мобільність;
- фінансування досліджень.

Чому моніторинг у сфері трансферту технологій є критично важливим

Трансфер технологій – це процес передачі знань, інновацій, програмного забезпечення, технічної документації або ноу-хау від наукової установи до зовнішнього середовища (бізнес, іноземні партнери, державні структури).

Разом із можливостями він створює ризики:

- незаконний експорт технологій подвійного призначення;
- порушення санкційних режимів;
- неправомірне розкриття інтелектуальної власності;
- витік конфіденційної інформації;
- недотримання умов грантів або контрактів;
- академічні та етичні порушення.

Тому моніторинг – це не лише контроль, а й механізм:

- запобігання правопорушенням;
- захисту репутації університету;
- забезпечення національної безпеки;
- підтримки академічної доброчесності.

Що таке моніторинг у сфері трансферту технологій

Моніторинг – це систематичний процес:

- спостереження,
- аналізу,
- перевірки,
- документування діяльності, пов’язаної з передачею технологій, з метою виявлення ризиків або порушень.

Він включає:

- юридичний контроль;
- фінансовий аудит;
- технічний аналіз;
- перевірку відповідності міжнародним режимам;
- аналіз поведінки контрагентів.

Основні види порушень у сфері трансферту технологій

1. Порушення експортного контролю

- передача технологій без ліцензії;
- співпраця з підсанкційними суб’єктами;
- участь у спільних проектах без узгодження;
- розкриття технічних деталей у відкритих публікаціях без перевірки.

2. Порушення прав інтелектуальної власності

- передача технології без реєстрації патенту;
- використання технології без дозволу власника;
- порушення умов ліцензійної угоди;
- привласнення результатів досліджень.

3. Контрактні порушення

- невиконання умов грантової угоди;
- неправомірне використання фінансування;
- передача технології третім особам без дозволу.

4. Етичні порушення

- прихований конфлікт інтересів;
- співпраця з сумнівними структурами;
- участь у проектах з високим ризиком подвійного призначення без належної оцінки.

Суб’єкти моніторингу

Моніторинг здійснюється на різних рівнях:

1. Внутрішній рівень (університет)

- відділ трансферу технологій;
- юридичний відділ;
- служба безпеки;
- комісії з етики;
- підрозділи внутрішнього аудиту.

2. Державний рівень

- органи експортного контролю;
- митні органи;
- правоохоронні органи;
- антикорупційні структури.

3. Міжнародний рівень

- організації контролю режимів нерозповсюдження;
- донорські фонди;
- міжнародні аудитори.

Механізми моніторингу

1. Документальний контроль

- перевірка договорів;
- аналіз ліцензій;
- аудит фінансових операцій;
- перевірка публікацій та технічної документації.

Це базовий рівень моніторингу.

2. Due Diligence (перевірка контрагентів)

Перед початком співпраці проводиться:

- аналіз структури власності;
- перевірка санкційних списків;
- оцінка репутаційних ризиків;
- аналіз попередньої діяльності партнера.

3. Внутрішні політики комплаєнсу

Університети впроваджують:

- кодекси поведінки;
- процедури погодження міжнародної співпраці;
- системи звітності;
- механізми анонімного повідомлення про порушення.

4. Технічний моніторинг

- контроль доступу до даних;
- журналювання передачі файлів;
- відстеження використання програмного забезпечення;
- контроль хмарних сервісів.

Інструменти виявлення порушень

1. Внутрішній аудит

Регулярні перевірки:

- контрактів;
- патентної активності;
- фінансових операцій;
- співпраці з іноземними партнерами.

2. Санкційні перевірки

Партнери перевіряються щодо:

- перебування під міжнародними санкціями;
- участі в незаконних схемах;
- зв’язків із забороненими структурами.

3. Аналіз аномалій

Наприклад:

- несподіване зростання міжнародних контрактів;
- незвичні фінансові транзакції;
- передача великого обсягу технічної інформації;
- активність, що не відповідає профілю дослідника.

Юридична відповідальність

Порушення можуть призвести до:

- адміністративної відповідальності;
- кримінальної відповідальності;
- фінансових санкцій;
- анулювання ліцензії;
- розірвання міжнародних угод;
- втрати грантового фінансування.

У серйозних випадках – міжнародні санкції.

Чому цифрові інструменти важливі

Сучасний трансфер технологій відбувається швидко, часто через:

- електронну пошту та хмарні сервіси;
- відкриті наукові платформи;
- програмне забезпечення та алгоритми, які можна передавати онлайн;
- цифрові конференції та віртуальні лабораторії.

Нелегальний експорт – це передача технологій або даних без відповідного дозволу або всупереч експортному контролю.

Цифрові інструменти допомагають:

- швидко виявляти потенційні порушення;
- відслідковувати аномальні потоки даних;
- документувати та створювати докази для юридичних процедур;
- підтримувати академічну доброчесність та безпеку наукових результатів.

Основні напрямки цифрового контролю

Аналіз електронного обігу даних

- контроль над відправкою документів і кодів;
- виявлення несанкціонованого доступу;
- відстеження підозрілих обсягів або адрес отримувачів.

Моніторинг публікацій та відкритих джерел

- перевірка наявності технічної інформації в наукових статтях;
- аналіз відкритих репозиторіїв коду;
- автоматичне порівняння публікацій з переліками контрольованих технологій.

Системи електронного ліцензування та реєстрації

- перевірка відповідності заявок на трансфер технологій;
- документування всіх дозволів і обмежень.

Аналітичні платформи та штучний інтелект

- аналіз шаблонів поведінки користувачів;
- прогноз ризиків нелегального експорту;
- автоматичне виявлення аномалій у трансферті даних.

Типи цифрових інструментів

Інструмент	Призначення	Приклади застосування
Системи моніторингу файлів	Відстеження передачі документів і програмного забезпечення	Логи серверів, DLP-системи (Data Loss Prevention)
Хмарні платформи з аудитом	Контроль доступу до даних у хмарі	Google Workspace, Microsoft 365 з аудитом активності
Аналітика на базі ШІ	Виявлення аномалій і ризикових операцій	Моделювання поведінки користувачів, аналіз патернів доступу
Репозиторії і системи контролю версій	Відстеження змін коду та документації	GitHub Enterprise з обмеженням доступу
Інструменти перевірки контрагентів	Перевірка партнерів та підрядників	Sanctions lists, корпоративні бази даних, AML-системи

Функціональні можливості цифрових систем

Контроль доступу – визначення, хто має право на використання або передачу технологій.

Логування дій – автоматична фіксація всіх операцій (завантаження, копіювання, пересилання).

Аналіз ризиків – системи оцінюють ймовірність порушення контролю експорту.

Попередження порушень – інструменти можуть блокувати потенційно небезпечні дії в режимі реального часу.

Звітність і аудит – забезпечення доказової бази для внутрішніх та державних перевірок.

Приклади цифрового моніторингу у наукових установах

Логування роботи з лабораторним обладнанням: відстежується, хто і коли проводив експерименти.

Контроль обміну кодом і моделями ШІ: блокування завантаження на зовнішні ресурси без дозволу.

Аналіз наукових публікацій: автоматичне порівняння змісту статей із переліками технологій подвійного призначення.

Моніторинг хмарних ресурсів: визначення аномальної передачі великих обсягів даних закордон.

Використання штучного інтелекту (ШІ) для виявлення порушень

Патерн-аналіз: алгоритми ШІ відстежують шаблони поведінки користувачів та визначають підозрілі дії.

Прогнозування ризиків: визначення високоризикових операцій і контрагентів.

Автоматичні сповіщення: система повідомляє адміністратора при спробі передачі заборонених технологій.

Переваги: швидкість, точність, зниження людського фактору.

Недоліки: можливі помилки, потреба у кваліфікованій настройці.

Переваги цифрових інструментів

- **Швидке виявлення порушень** у реальному часі;
- **Документування доказів** для внутрішнього аудиту та державного контролю;
- **Підвищення культури безпеки** серед науковців;
- **Зниження ризику юридичної відповідальності** для установ і дослідників;
- **Сумісність із міжнародними режимами контролю** (Wassenaar Arrangement, MTCR, NSG).

Виклики та обмеження

- Потрібне **технічне забезпечення** та фахівці;
- Ризик **помилкового блокування легальних дій**;
- Питання **конфіденційності та академічної свободи**;
- Постійне оновлення баз даних та алгоритмів через зміну переліків контрольованих технологій.

ЖИТОМИРСЬКА ПОЛІТЕХНІКА
ДЕРЖАВНИЙ УНІВЕРСИТЕТ

@ZTUEDUUA

ДЯКУЮ ЗА УВАГУ!!!