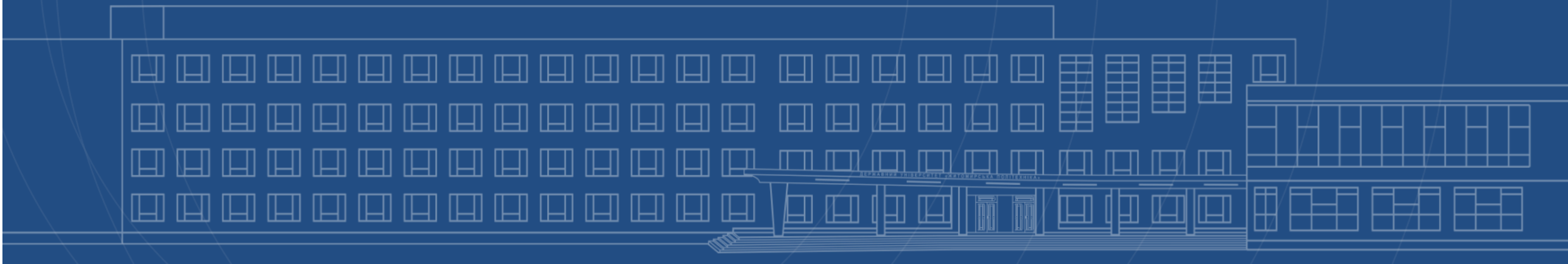
ЖИТОМИРСЬКА ПОЛІТЕХНІКА
ДЕРЖАВНИЙ УНІВЕРСИТЕТ

@ZTUEDUUA

ТЕМА 6. ІНФОРМАЦІЙНА ГІГІЄНА ДОСЛІДНИКА ТА ЗАХИСТ НАУКОВИХ ДАНИХ

План

1. Безпека зберігання та резервування результатів наукових досліджень
2. Захист даних при використанні хмарних сервісів і міжнародних цифрових платформ
3. Безпечне використання спеціалізованого програмного забезпечення та інформаційних систем
4. Обмеження використання інформації з джерел держави-агресора
5. Контроль застосування штучного інтелекту для забезпечення академічної доброчесності



Збереження результатів дослідження – це не технічна проблема, а складова професійної відповідальності дослідника.

Втрата результатів дослідження означає втрату:

- доказової бази дисертації;
- можливості повторної перевірки;
- аргументів у науковій дискусії;
- прав на інтелектуальну власність.

До результатів дослідження належать:

- первинні емпіричні матеріали (анкети, інтерв’ю, експертні висновки);
- статистичні таблиці;
- протоколи спостережень;
- робочі версії текстів;
- бази даних;
- аудіо- та відеоматеріали;
- службове листування щодо дослідження;
- грантові документи.

Основні ризики втрати наукових результатів

1. **Людський фактор**: випадкове видалення; втрата ноутбука; використання ненадійних носіїв.
2. **Організаційні проблеми**: відсутність системного підходу до зберігання; зберігання лише на особистому пристрої.
3. **Цифрові загрози**: вірусні атаки; блокування файлів; витік конфіденційної інформації.
4. **Фізичні фактори**: пожежа; затоплення; технічна несправність.

Наявність системно збережених матеріалів дозволяє:

- довести авторство;
- підтвердити пріоритет ідеї;
- захистити результати у випадку спору;
- виконати умови грантової угоди;
- підтвердити коректність використання персональних даних.

Особливої уваги потребують дослідження, що містять:

- персональні дані;
- чутливу інформацію;
- медичні або соціологічні матеріали;
- експертні висновки.

У таких випадках збереження має враховувати:

- конфіденційність;
- згоду учасників;
- обмеження доступу;
- терміни зберігання.

Недбале зберігання може призвести до юридичної відповідальності.

Організаційна культура зберігання даних

У науковій установі повинні бути:

- внутрішні регламенти зберігання;
- централізовані сховища;
- чітке розмежування доступу;
- періодичне резервування;
- визначення відповідальних осіб.

Збереження не може бути приватною справою здобувача – це інституційна політика.

Внутрішня політика безпеки дослідника включає:

- регулярне створення резервних копій;
- використання складних паролів;
- обмеження доступу до конфіденційних матеріалів;
- ведення обліку версій документів;
- порядок передачі матеріалів через незахищені канали

Сучасна наукова діяльність неможлива без використання:

- хмарних сховищ;
- міжнародних репозитаріїв;
- цифрових платформ спільної роботи;
- систем онлайн-рецензування;
- міжнародних баз даних.

Хмарний сервіс – це віддалена інфраструктура зберігання або обробки даних, доступ до якої здійснюється через Інтернет.

Для аспірантів це означає:

- зберігання матеріалів на Google Drive або OneDrive;
- спільне редагування документів;
- зберігання баз даних на зовнішніх серверах;
- використання платформ для статистичної обробки.

Ключова особливість: фізично дані зберігаються не у дослідника, а на серверах третьої сторони.

Переваги хмарних сервісів для науки

1. Доступність з будь-якої точки світу.
2. Спільна робота кількох авторів.
3. Автоматичне резервування.
4. Масштабованість.
5. Інтеграція з міжнародними науковими платформами.

Ризики використання хмарних сервісів

- передача даних за межі національної юрисдикції;
- обмежений контроль над фізичним розміщенням серверів;
- можливість несанкціонованого доступу;
- витік персональних або конфіденційних даних;
- залежність від політики провайдера.

Використання хмарних сервісів має враховувати:

- права респондентів;
- очікування конфіденційності;
- прозорість дослідницького процесу;
- принцип мінімізації даних.

Для мінімізації ризиків доцільно:

- використовувати офіційні університетські акаунти;
- не зберігати чутливі дані у публічних папках;
- застосовувати розмежування доступу;
- регулярно переглядати права користувачів;
- створювати локальні резервні копії.

Рекомендована стратегія безпечного використання хмари

1. Використання офіційних акаунтів.
2. Розділ відкритих та конфіденційних матеріалів.
3. Збереження локальної копії.
4. Обмеження доступу за принципом необхідності.
5. Перевірка політики конфіденційності сервісу.

Інформаційна гігієна – це сукупність знань, навичок і правил поведінки дослідника у цифровому середовищі, спрямованих на:

- захист наукових даних;
- збереження конфіденційності;
- забезпечення академічної доброчесності;
- мінімізацію цифрових ризиків;
- правомірне використання інформаційних ресурсів.

Інформаційна гігієна – це не технічна компетенція програміста, а елемент професійної відповідальності дослідника, що впливає на якість наукової роботи, її легітимність та репутацію автора.

Спеціалізоване програмне забезпечення в науковій діяльності: що ми використовуємо

У науковій роботі застосовуються:

1. Статистичні програми – для обробки кількісних даних;
2. Програми для якісного аналізу – аналіз інтерв’ю, текстів.
3. Бібліографічні менеджери – управління джерелами.
4. Онлайн-платформи опитувань.
5. Хмарні сервіси для зберігання.
6. Системи перевірки на плагіат.
7. Академічні бази даних.

Неправильне використання програм може призвести до:

- втрати первинних даних;
- некоректної обробки інформації;
- маніпулятивної інтерпретації результатів;
- витоку персональних даних респондентів;
- порушення ліцензійного законодавства.

Ризики при використанні спеціалізованого ПЗ

1. Технічні ризики

- збої системи;
- вірусні атаки;
- пошкодження файлів.

2. Організаційні ризики

- передача доступу стороннім особам;
- зберігання даних без резервування;
- відсутність політики безпеки.

3. Правові ризики

- обробка персональних даних без належного захисту;
- використання неліцензійного ПЗ;
- порушення умов користування платформами.

Використання ліцензійного програмного забезпечення:

- гарантує технічну підтримку;
- забезпечує оновлення безпеки;
- мінімізує ризик вбудованого шкідливого коду;
- захищає університет від юридичних претензій.

Неліцензійне ПЗ:

- може містити приховані програми збору даних;
- порушує авторські права;
- підриває академічну етику.

Основні правила безпечного використання акаунтів і управління доступом:

- складні унікальні паролі;
- двофакторна автентифікація;
- обмеження спільного доступу;
- регулярна перевірка активних сесій.

Більшість витоків інформації відбувається через компрометацію облікових записів, а не через складні хакерські атаки.

Безпечне використання бібліографічних менеджерів

Переваги:	Ризики:
- **автоматизація;** - **економія часу;** - **точність цитування.**	- синхронізація з хмарою; - автоматичний обмін бібліотеками; - збереження PDF-файлів на сторонніх серверах.
Рекомендації: - **перевіряти налаштування приватності;** - **не зберігати конфіденційні матеріали у відкритих групах**	

В умовах збройної агресії та гібридної війни інформація стає інструментом впливу, маніпуляції та дестабілізації.

Для науковця це означає:

- підвищений ризик використання недостовірних джерел;
- можливість несвідомого поширення пропагандистських наративів;
- репутаційні ризики;
- правові наслідки використання заборонених ресурсів.

Інформаційна гігієна передбачає критичну оцінку походження джерела та його правового статусу.

Джерелами держави-агресора є:

- офіційні органи влади держави-агресора;
- підконтрольні медіа;
- наукові установи, що працюють в умовах державної пропаганди;
- цифрові платформи, що підтримують політику агресії;
- інформаційні ресурси, внесені до санкційних списків.

Йдеться не лише про політичну позицію, а про системний характер інформаційного впливу.

Інформаційна сфера є частиною національної безпеки.

Для дослідника це означає:

- необхідність враховувати контекст походження інформації;
- недопущення легітимізації пропагандистських наративів;
- розуміння, що наука також є об’єктом інформаційної війни.

Нормативно-правові обмеження базуються на:

- санкційному законодавстві;
- рішеннях органів державної влади щодо блокування ресурсів;
- внутрішніх політиках університетів;
- правилах грантових програм та міжнародних фондів.

Порушення таких обмежень може мати дисциплінарні або юридичні наслідки.

Використання джерел країни-агресора є проблемним через:

1. Ризик маніпуляції фактами.
2. Використання перекручених статистичних даних.
3. Відсутність академічної незалежності авторів.
4. Поширення ідеологічних конструктів під виглядом наукових досліджень.

Використання сумнівних джерел:

- знижує довіру до роботи;
- ставить під сумнів академічну доброчесність;
- створює негативний імідж у міжнародному середовищі;
- ускладнює публікацію у фахових журналах.

Етичний вимір проблеми

Науковець є:

- суб’єктом академічної спільноти;
- носієм професійної етики;
- відповідальним за наслідки своїх досліджень.

Використання джерел держави-агресора – це не лише технічне, а й моральне питання.

Інструменти штучного інтелекту (ШІ) в академічному середовищі – потужного інструменту, який дозволяє:

- пришвидшувати роботу,
- допомагати структурувати матеріал,
- покращувати мовне оформлення,
- сприяти пошуку ідей.

ШІ створює нові виклики для академічної доброчесності, оскільки межа між допомогою і підміною авторської роботи стає менш очевидною.

Інформаційна гігієна дослідника в умовах використання ШІ полягає у вмінні:

- усвідомлено застосовувати цифрові інструменти,
- контролювати їх вплив на результат,
- не перекладати відповідальність на алгоритм.

Академічна доброчесність традиційно базується на принципах:

- самостійності виконання дослідження,
- достовірності результатів,
- коректності цитування,
- відповідальності за зміст роботи.

Застосування ШІ не скасовує цих принципів. Навпаки, воно потребує їх більш чіткого усвідомлення.

Межа між допустимою допомогою та недоброчесною практикою

Допустиме використання:

- перевірка граматики та стилю;
- технічне редагування;
- допомога у структуризації матеріалу;
- формування переліку можливих напрямів пошуку літератури;
- уточнення термінології.

Недопустиме використання:

- автоматичне написання розділів дисертації;
- генерування теоретичних положень без їх глибокого осмислення;
- створення висновків, які автор не здатен пояснити;
- формування вигаданих джерел;
- створення або модифікація дослідницьких результатів.

Проблема фабрикації джерел та псевдонаукової інформації

Один із найбільших ризиків застосування ШІ – створення так званих «галюцинацій», тобто вигаданих фактів, статей або посилань.

Алгоритм може:

- сформувати назву неіснуючої статті;
- приписати її реальному автору;
- вказати неіснуючий журнал або рік публікації.

Інформаційна гігієна передбачає обов’язкову верифікацію кожного джерела через офіційні наукові бази даних.

Більшість сервісів ШІ працюють через онлайн-платформи. Це означає, що:

- введений текст може зберігатися на серверах компанії;
- дані можуть використовуватися для навчання алгоритмів;
- існує ризик несанкціонованого доступу.

Особливо небезпечно вводити:

- неопубліковані результати дисертації;
- персональні дані респондентів;
- конфіденційну інформацію партнерів.

Захист наукових даних є частиною професійної відповідальності дослідника.

З метою здійснення інституційного контролю університети / наукові установи впроваджують:

- політики декларування використання ШІ;
- правила допустимого застосування;
- рекомендації щодо прозорості;
- механізми перевірки.

Метою контролю є не заборона технологій, а забезпечення чесності процесу навчання і дослідження.

Незалежно від ступеня використання ШІ, автор несе відповідальність за:

- достовірність фактів,
- коректність інтерпретації,
- логічність аргументації,
- відповідність етичним стандартам
- завжди несе автор.

Використання ШІ піднімає низку етичних питань:

- Чи не знецінює це інтелектуальну працю?
- Чи не створює це нерівні умови між дослідниками?
- Чи не підміняє це процес навчання?

Інформаційна гігієна включає здатність ставити такі питання і шукати збалансовані рішення.

ЖИТОМИРСЬКА ПОЛІТЕХНІКА
ДЕРЖАВНИЙ УНІВЕРСИТЕТ

@ZTUEDUUA

ДЯКУЮ ЗА УВАГУ!!!