ЖИТОМИРСЬКА ПОЛІТЕХНІКА
ДЕРЖАВНИЙ УНІВЕРСИТЕТ

@ZTUEDUUA

ТЕМА 8. ПОЛІТИКА ІНФОРМАЦІЙНОЇ БЕЗПЕКИ ДЛЯ УСТАНОВ, ЩО ЗДІЙСНЮЮТЬ НАУКОВУ ДІЯЛЬНІСТЬ

План

1. Сфера застосування та структура політики інформаційної безпеки
2. Документальне забезпечення політики інформаційної безпеки.
3. Due Diligence у наукових проєктах і міжнародній співпраці
4. Політика інформаційної безпеки в наукових установах та закладах вищої освіти

Політика інформаційної безпеки – це офіційний нормативний документ установи, який визначає:

- принципи захисту інформації;
- правила роботи з даними;
- розподіл відповідальності;
- механізми запобігання порушенням;
- порядок реагування на інциденти.

Для наукової установи політика інформаційної безпеки – це не лише технічний документ, а:

- управлінський інструмент;
- елемент системи внутрішнього контролю;
- засіб захисту інтелектуальної власності;
- гарантія відповідності законодавству;
- складова академічної доброчесності.

Наукові установи мають специфіку:

- **Великий обсяг унікальних даних**
  - результати досліджень;
  - експериментальні масиви;
  - програмний код;
  - аналітичні моделі;
  - рукописи та неопубліковані матеріали.
- **Міжнародна співпраця**
  - спільні проєкти;
  - обмін даними;
  - доступ до міжнародних платформ.
- **Грантове фінансування**
  - вимоги донорів щодо безпеки;
  - контроль використання коштів.
- **Технології подвійного призначення**
  - ризик експортних обмежень;
  - державний контроль.

Політика повинна чітко визначати:

1. Суб’єктів (керівництво установи; наукових працівників; аспірантів; адміністративний персонал; ІТ-служби; зовнішніх підрядників; запрошених дослідників);

2. Об’єкти захисту (наукові дані (опубліковані та неопубліковані); бази даних та архіви; інтелектуальна власність; персональні дані учасників досліджень; грантова документація; лабораторне програмне забезпечення; сервери та хмарні ресурси);

3. Територіальне та цифрове охоплення (приміщення установи; віддалений доступ; хмарні платформи; мобільні пристрої; міжнародні партнерські мережі).

Основні цілі політики інформаційної безпеки

- Забезпечення **конфіденційності** (захист від несанкціонованого доступу).
- Гарантування **цілісності** (захист від спотворення або знищення даних).
- Підтримка **доступності** (збереження безперервності досліджень).
- Виконання **законодавчих вимог**.
- Запобігання витоку технологій.
- Підтримка академічної доброчесності.

Структура політики інформаційної безпеки

1. Загальні положення (мета документа; правові підстави; сфера застосування; термінологія);

2. Принципи інформаційної безпеки (законність; відповідальність; мінімізація доступу; пропорційність заходів; прозорість процедур; баланс безпеки та академічної свободи.

3. Класифікація інформації

Рівень	Характеристика	Приклад
Відкрита	Може публікуватися без обмежень	Статті після рецензування
Службова	Для внутрішнього використання	Робочі звіти
Конфіденційна	Обмежений доступ	Дані експериментів
Особливо чутлива	Високий рівень захисту	Дані подвійного призначення

4. Управління доступом (процедури надання доступу; принцип «мінімальної необхідності»; багаторівнева автентифікація; регулярний перегляд прав доступу;

5. Захист інформаційних систем (вимоги до програмного забезпечення; резервне копіювання; антивірусний захист; оновлення систем);

6. Управління ризиками (ідентифікація ризиків; оцінка ймовірності; визначення наслідків; заходи мінімізації)

7. Реагування на інциденти (порядок повідомлення; фіксація доказів; внутрішнє розслідування; взаємодія з правоохоронними органами);

8. Навчання та підвищення обізнаності (обов’язкові інструктажі; курси для аспірантів; регулярні оновлення політики.

Політика має багаторівневу структуру:

1. **Базова політика** — стратегічний документ.
2. **Процедури** — опис конкретних процесів.
3. **Інструкції** — покрокові правила.
4. **Регламенти** — відповідальність та строки.
5. **Форми звітності** — журнали, акти, протоколи.

Політика інформаційної безпеки повинна узгоджуватися з:

- Законом України «Про інформацію»;
- Законом України «Про захист інформації в інформаційно-телекомунікаційних системах»;
- Законом України «Про наукову і науково-технічну діяльність»;
- Законом України «Про захист персональних даних»;
- законодавством про державну таємницю;
- міжнародними вимогами донорів і грантодавців.

Ризики відсутності або формального характеру політики інформаційної безпеки

- витік результатів досліджень;
- втрата грантів;
- міжнародні санкції;
- юридична відповідальність;
- репутаційні втрати;
- блокування міжнародної співпраці.

Документальне забезпечення політики інформаційної безпеки – це сукупність внутрішніх нормативних, організаційних і процедурних документів, які:

- формалізують правила захисту інформації;
- визначають відповідальність посадових осіб;
- регламентують порядок доступу, використання та передачі даних;
- створюють доказову базу у випадку перевірок або інцидентів.

У науковій установі документація має особливе значення, оскільки:

- дослідження часто пов’язані з інтелектуальною власністю;
- можливий експорт технологій;
- існують міжнародні зобов’язання;
- працюють аспіранти та зовнішні партнери.

Ієрархія документів у сфері інформаційної безпеки

Рівень 1 – Стратегічні документи (Політика інформаційної безпеки, Стратегія цифрового розвитку; Положення про систему внутрішнього контролю);

Рівень 2 – Організаційно-нормативні документи (Положення про захист інформації; Положення про порядок доступу до інформаційних систем; Положення про захист персональних даних; Положення про трансфер технологій; Положення про експортний контроль);

Рівень 3 – Процедурні документи (Інструкція з резервного копіювання; Інструкція з роботи з конфіденційною інформацією; Порядок реагування на інциденти; Регламент надання доступу; Порядок перевірки контрагентів);

Рівень 4 – Операційні документи (Журнали доступу; Акти приймання-передачі даних; Протоколи інструктажу; Звіти про аудит; Реєстри носіїв інформації).

Основні види документів у науковій установі

1. Політика інформаційної безпеки (затверджується наказом керівника; має обов’язковий характер; поширюється на всіх працівників);

2. Положення про конфіденційну інформацію (визначає: категорії інформації; порядок маркування; правила зберігання; відповідальність за порушення);

3. Договори та угоди (угода про нерозголошення (NDA); трудовий договір із положеннями про конфіденційність; договори з підрядниками; грантові угоди);

4. Регламенти доступу (містять: процедуру подання заявки; критерії надання доступу; строки дії доступу; порядок відкликання);

5. Документи щодо реагування на інциденти (план реагування; акт фіксації порушення; звіт про розслідування; рішення дисциплінарної комісії).

Документування процесів експортного контролю

- внутрішній порядок перевірки трансферу технологій;
- перелік контрольованих технологій;
- журнал міжнародних передач;
- процедуру узгодження з державними органами.

Типові помилки у документальному забезпеченні

- Формальне копіювання шаблонів без адаптації.
- Відсутність оновлення документів.
- Невідповідність фактичної практики задекларованим правилам.
- Відсутність доказів проведення інструктажів.
- Неузгодженість між різними положеннями.

Due Diligence (належна обачність) – це комплексна перевірка контрагентів, партнерів, проєктів та ризиків перед укладенням договорів або початком співпраці.

У науковій діяльності Due Diligence означає:

- оцінку правових, фінансових та репутаційних ризиків;
- перевірку відповідності експортному контролю;
- аналіз доброчесності партнерів;
- перевірку джерел фінансування;
- забезпечення дотримання вимог безпеки.

Це не лише юридична процедура, а інструмент стратегічного управління ризиками.

Чому Due Diligence критично важливий для наукових установ

Наукові установи працюють у середовищі:

- міжнародної кооперації;
- трансферу технологій;
- грантового фінансування;
- публікації результатів;
- роботи з чутливими даними.

Без належної перевірки можливі:

- порушення санкційного режиму;
- незаконний експорт технологій;
- фінансування з небезпечних джерел;
- співпраця з недоброчесними структурами;
- репутаційні втрати.

Основні цілі Due Diligence

- Виявлення правових ризиків.
- Запобігання витоку технологій.
- Захист інтелектуальної власності.
- Дотримання міжнародних режимів експортного контролю.
- Перевірка академічної доброчесності.
- Забезпечення відповідності грантовим вимогам.

Сфера застосування у науковій діяльності

- Due Diligence застосовується при:
- укладенні міжнародних договорів;
- створенні спільних лабораторій;
- передачі технологій;
- публікації досліджень із подвійним призначенням;
- отриманні грантів;
- закупівлі обладнання;
- залученні іноземних дослідників.

Основні види Due Diligence

1. Юридичний Due Diligence (перевіряється: правовий статус партнера; повноваження підписантів; судові спори; відповідність санкційному законодавству; дотримання експортного контролю);

2. Фінансовий Due Diligence (оцінюється: джерело фінансування; прозорість фінансової діяльності; ризики відмивання коштів; фінансова стабільність партнера);

3. Репутаційний Due Diligence (перевіряється: академічна доброчесність; участь у скандалах; зв’язки з державами-агресорами; відповідність етичним стандартам);

4. Технологічний Due Diligence (аналізується: характер технології; можливість подвійного використання; рівень секретності; ризики незаконного експорту; потенційна військова або стратегічна значущість).

Процедура проведення Due Diligence

Етап 1. Ідентифікація партнера **(офіційна назва; країна реєстрації; структура власності; кінцеві бенефіціари;**

Етап 2. Аналіз відкритих джерел **(офіційні реєстри; санкційні списки; публічні бази даних; наукові публікації);**

Етап 3. Оцінка ризиків **(геополітичні ризики; правові обмеження; технологічна чутливість);**

Етап 4. Прийняття управлінського рішення **(дозвіл на співпрацю; додаткові гарантії; відмова від співпраці.**

Інструменти Due Diligence

- Санкційні списки (OFAC, ЄС, національні списки).
- Бази даних корпоративної інформації.
- Платформи перевірки бенефіціарів.
- Системи експортного контролю.
- Внутрішні реєстри ризиків.
- Цифрові аналітичні системи.

Типові ризики при відсутності Due Diligence

- співпраця з підсанкційними установами;
- порушення експортного законодавства;
- втрати грантів;
- витік чутливої інформації;
- міжнародні скандали;
- кримінальна відповідальність.

Due Diligence не повинен:

- обмежувати свободу наукового пошуку;
- створювати надмірну бюрократію;
- блокувати легітимну міжнародну співпрацю.

Але він повинен:

- мінімізувати ризики;
- захищати інтереси держави;
- гарантувати правову безпеку дослідників.

Університети та наукові установи є складними організаціями, що поєднують:

- освітню діяльність;
- наукові дослідження;
- міжнародну співпрацю;
- трансфер технологій;
- цифрову інфраструктуру.

Політика інформаційної безпеки – це стратегічний документ, який:

- визначає правила роботи з інформацією;
- регламентує захист наукових результатів;
- встановлює відповідальність;
- забезпечує відповідність законодавству;
- мінімізує ризики витоку технологій.

Особливості наукових і освітніх установ як об’єктів захисту

1. Працюють з великим обсягом відкритих даних (публікації, репозитарії).
2. Паралельно мають конфіденційну інформацію (неопубліковані дослідження, гранти).
3. Забезпечують доступ тисячам користувачів (студенти, аспіранти, викладачі).
4. Здійснюють міжнародну співпрацю.
5. Працюють із персональними даними.

Цілі політики інформаційної безпеки

1. Захист конфіденційної інформації.
2. Забезпечення цілісності наукових даних.
3. Підтримка безперервності освітнього процесу.
4. Виконання законодавчих вимог.
5. Захист інтелектуальної власності.
6. Запобігання кіберінцидентам.
7. Забезпечення академічної доброчесності.

Принципи інформаційної безпеки в університеті

- законності;
- пропорційності;
- мінімізації доступу;
- відповідальності;
- прозорості процедур;
- балансу безпеки та академічної свободи;
- регулярного перегляду ризиків.

Політика інформаційної безпеки поширюється на:

- *Суб'єктів:* керівництво; науковців; викладачів; аспірантів; студентів; адміністративний персонал; ІТ-служби; зовнішніх партнерів.
- *Об'єкти захисту:* результати досліджень; грантові матеріали; електронні бази даних; лабораторні системи; персональні дані; сервери і хмарні ресурси; освітні платформи.

Структура політики інформаційної безпеки

1. Загальні положення (мета; сфера дії; правові підстави; термінологія)

2. Класифікація інформації (публічна – відкрита інформація; службова – внутрішня інформація; конфіденційна – обмежений доступ; чутлива – підвищений рівень захисту);

3. Управління доступом (принцип мінімальної необхідності; автентифікація користувачів; періодичний перегляд прав доступу; контроль віддаленого доступу);

4. Захист інформаційних систем (резервне копіювання; оновлення програмного забезпечення; антивірусний захист; аудит та моніторинг; захист хмарних ресурсів);

5. Управління ризиками (включає: ідентифікацію ризиків; оцінку впливу; визначення заходів мінімізації; регулярний перегляд);

6. Реагування на інциденти (Політика повинна містити: порядок повідомлення; процедуру розслідування; фіксацію доказів; комунікацію із зовнішніми органами; відновлення систем).

Інформаційна безпека пов’язана з:

- запобіганням плагіату;
- захистом авторських прав;
- контролем використання штучного інтелекту;
- захистом даних досліджень;
- запобіганням фальсифікаціям.

Установі доцільно передбачити:

- відповідального за інформаційну безпеку;
- комісію з кібербезпеки;
- службу внутрішнього аудиту;
- відділ трансферу технологій;
- підрозділ захисту персональних даних.

Типові ризики для ЗВО та наукових установ

- Кібератаки.
- Витік неопублікованих досліджень.
- Несанкціонований експорт технологій.
- Порушення захисту персональних даних.
- Використання неліцензійного ПЗ.
- Співпраця з підсанкційними організаціями.

Баланс відкритості науки і безпеки

Політика інформаційної безпеки повинна:

- не обмежувати академічну свободу;
- забезпечувати відкриту науку;
- водночас захищати чутливі технології;
- гарантувати відповідність законодавству.

ЖИТОМИРСЬКА ПОЛІТЕХНІКА
ДЕРЖАВНИЙ УНІВЕРСИТЕТ

@ZTUEDUUA

ДЯКУЮ ЗА УВАГУ!!!