УПРАВЛІННЯ КІБЕРБЕЗПЕКОЮ В ОСВІТНІЙ ТА НАУКОВІЙ ДІЯЛЬНОСТІ

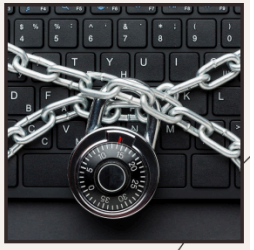
Кафедра інноваційних та інформаційних технологій в освіті

Компетентності	Результати навчання	Форми освітнього процесу	Види навчальних занять	Види навчальної діяльності	Методи, технології викладання навчання	Засоби навчання	Методи та критерії оцінювання
1	2	3	4	5	6	7	8
−Здатність обґрунтовувати, аналізувати і розробляти адекватні інтелектуальні методи для систем кіберзахисту. − Здатність обґрунтовувати вибір програмного забезпечення, устаткування та інструментів в галузі інформаційної безпеки та/або кібербезпеки на основі сучасних інтелектуальних методів систем штучного інтелекту. − Здатність здійснювати дослідження у галузі інформаційної безпеки та/або кібербезпеки із застосуванням сучасних інтелектуальних методів моделювання складних процесів та систем штучного інтелекту.	− Застосовувати методи систем штучного інтелекту для розробки та удосконалення сучасних інформаційних технологій та математичних методів і моделей інтелектуальних систем в сфері інформаційної безпеки та/або кібербезпеки. − Застосовувати, інтегрувати, розробляти, впроваджувати та удосконалювати сучасні інформаційні технології, фізичні та математичні методи і моделі в сфері інформаційної безпеки та/або кібербезпеки. − Обирати, аналізувати і розробляти придатні типові аналітичні, розрахункові та експериментальні методи кіберзахисту, розробляти, реалізовувати та супроводжувати проєкти з захисту інформації у кіберпросторі, інноваційної діяльності та захисту інтелектуальної власності.	Навчальні заняття, самостійна робота, контрольні заходи.	Лекційні, лабораторні заняття.	Групова робота на лабораторних заняттях, моделювання; публічний виступ; робота в малих групах; ситуаційні завдання.	Проблемнопошуковий метод, навчальна дискусія (дебати), мозковий штурм, аналіз ситуації. Імітаційні технології (ігрові – рольові та ділові ігри, навчальні ігри, неігрові – аналіз конкретних ситуацій, розв’язання винахідницьких завдань) .	Об’єкти навколишнього середовища, діючі моделі, технічні засоби; мультимедіа-, відео-, звуковідтворююча, проекційна апаратура; комп’ютери, інформаційно-комунікаційні системи, бібліотечні фонди.	Усні, письмові відповіді, презентації, тестування, наукові проекти, захист індивідуальної/командної роботи. ***Критерії оцінювання:*** виконання роботи у визначений термін, виконання роботи відповідно до вимог (повнота викладу, стиль викладу, наявність сучасних джерел, іншомовних джерел, використання статистики; пояснення щодо застосування методів дослідження; власний аналіз та узагальнення; обґрунтовані висновки тощо); аргументи на захист результатів роботи, формування відповідей на запитання тощо.

УПРАВЛІННЯ КІБЕРБЕЗПЕКОЮ В ОСВІТНІЙ ТА НАУКОВІЙ ДІЯЛЬНОСТІ

Важливість кібербезпеки

Забезпечення **кібербезпеки** в освітніх установах є *важливою* складовою сучасної освіти. Захист від **кіберзагроз** дозволяє зберегти конфіденційність та цілісність даних, а також запобігти негативним наслідкам для навчального процесу.



Технологічні виклики

Зростання використання *інформаційних технологій* у навчальних закладах створює нові **виклики** для кібербезпеки. Підвищення **свідомості** та впровадження **заходів захисту** даних є необхідними для вирішення цих проблем.

Створення безпечної атмосфери

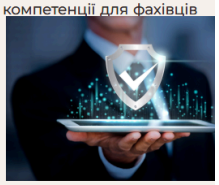
Створення **безпечної** кіберпростору в навчальних закладах потребує комплексного підходу. Важливо проводити **навчання** та надавати **інструменти** для захисту від **кіберзагроз**.

Зміст дисципліни

1. Порівняльний аналіз міжнародних стандартів та української нормативної бази в частині управління інцидентами інформаційної безпеки
2. Системи управління кібербезпекою
3. Основи планування безперервності роботи державних інформаційно-комунікаційних
систем
4. Система управління інцидентами інформаційної безпеки
5. Принципи збору інформації для системи виявлення і блокування атак

Компетенції

Компетенції управління кібербезпекою в освітніх закладах включають широкий спектр навичок і знань, необхідних для ефективного захисту
інформації та мережевих ресурсів. Ось деякі ключові компетенції для фахівців з
управління кібербезпекою в освітніх закладах:



1. Розуміння загроз і вразливостей
2. Стратегічне планування
3. Розробка політик та процедур
4. Технічна експертиза
5. Управління ризиками
6. Комунікаційні навички
7. Системний підхід: Здатність думати системно та розглядати кібербезпеку як інтегровану частину загальної стратегії управління ризиками.

Ці компетенції є важливими для забезпечення ефективного управління кібербезпекою в освітніх закладах та забезпечення безпеки інформації та мережевих ресурсів.