

ОСНОВИ КІБЕРБЕЗПЕКИ

Кафедра цифрових технологій і професійної освіти

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 усвідомлювати типові загрози, атаки та галузі їх розповсюдження, класифікувати проблеми захисту даних та засоби протидії злочинності. – Здатність розрізняти алгоритми шифрування, методи аутентифікації, авторизації та ідентифікації користувачів. – Здатність класифікувати основні кіберзакони, стандарти та відповідальність, основні типи засобів контролю цілісності даних, технології реагування на інциденти.	– Ідентифікувати можливі загрози та атаки. – Налаштовувати локальну та групову політику безпеки системи. – Налаштовувати безпеку локальної мережі. – Шифрувати конфіденційні дані стандартними алгоритмами шифрування. – Налаштовувати безпеку веббраузера. – Користуватися цифровим підписом. – Налаштовувати брандмауер. – Налаштовувати базову безпеку на маршрутизаторі. – Застосовувати знання з кібербезпеки у практичній діяльності.	Навчальні заняття, самостійна робота, контрольні заходи .	Лекційні, лабораторні заняття.	Груповою роботою на лабораторних заняттях, моделювання; публічний виступ; робота в малих групах; ситуативна вправа.	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 питання тощо.



Основи Кібербезпеки

Кібербезпека - **важлива** складова сучасного світу. Вона забезпечує захист **інформації** та інфраструктури від **кіберзагроз**. Ця галузь швидко розвивається та має великі **перспективи**.

Кібербезпека - це сукупність заходів, які спрямовані на захист інформації, комп'ютерних систем, мереж та інфраструктури від кіберзагроз.



Загрози в Інтернеті

У світі Інтернету існує багато **загроз**. Це можуть бути **віруси**, **шахраї**, **фішинг** та інші. Важливо бути **пильними** та захищати свою **інформацію**.



Засоби Захисту

Для захисту від кіберзагроз використовуються **програмні та апаратні засоби**. Це можуть бути **антивіруси, файерволи, шифрування та інші технології**.



Зміст дисципліни

1. Законодавча та нормативно-правова база України в галузі інформаційної та/або кібербезпеки. Закон України «Про освіту».
2. Основні міри протидії загрозам безпеці, принципи побудови систем захисту, основні механізми захисту
3. Інструментальні та прикладні застосунки в інформаційній та/або кібербезпеці
4. Контроль, автентифікація, авторизація та облік в операційних системах
5. Комп'ютерні мережі та безпека

Навчання кібербезпеці включає в себе різноманітні аспекти, такі як відповідальне використання Інтернету, основи кібергігієни, знання про шкідливе програмне забезпечення та методи захисту від нього, а також вивчення кібератак і способів їх запобігання. Збільшення кіберосвіти допомагає зменшити ризики кіберзлочинності та підвищує загальний рівень кібербезпеки в суспільстві.



Викладач:

доц. Уманець В. О.