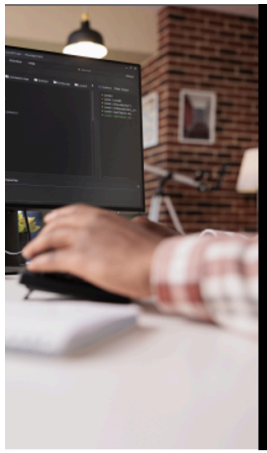
ЗАХИСТ ІНФОРМАЦІЇ В КОМП'ЮТЕРНИХ СИСТЕМАХ І МЕРЕЖАХ

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 уявлення про призначення, структуру та принципи побудови захищених інформаційних і комунікаційних систем, методи та моделі захисту інформації. − Здатність розрізняти сучасні способи боротьби з несанкціонованим блокуванням, копіюванням, зміною та збором інформації; програмні засоби забезпечення інформаційної безпеки. − Здатність класифікувати основні принципи, методи й алгоритми експлуатації програмних систем збору, закриття, відновлення і автентифікації інформації.	− Практично вирішувати завдання захисту програм та даних в комп'ютерних системах та мережах програмно-апаратними засобами та давати оцінку якості прийнятих рішень. – Практично вирішувати завдання захисту в операційних системах та давати оцінку якості прийнятих рішень. – Реалізовувати системи захисту інформації в ІКС відповідно до стандартів з оцінки захищених систем. – Реалізовувати захист інформації в системах передачі даних та системах зв'язку. – Користуватися науковою та довідковою літературою за напрямком дисципліни.	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 проєкти, 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.



Захист інформації в комп’ютерних системах і мережах

Вступ

Кібербезпека в Україні відіграє *важливу* роль у захисті інформації та інфраструктури від кіберзагроз. Це стає все більш актуальним в контексті зростаючих кібератак та проникнень у системи.

Тенденції

Збільшення обсягу кіберзлочинності та шпигунства. Зростання кількості кібератак на державні та комерційні інформаційні системи. Необхідність посилення заходів з кіберзахисту.

ЗМІСТ

Вивчення кібербезпеки є важливим для навчання ефективних методів захисту від кіберзагроз у цифровій епохі. Це допомагає захищати особисті дані, фінансові активи, корпоративні інформаційні ресурси та забезпечує безпеку національної інфраструктури. Крім того, вивчення кібербезпеки сприяє підвищенню свідомості про ризики кіберзлочинності та підготовці кваліфікованих фахівців, які можуть відповідати на сучасні виклики цифрової безпеки.

Комплексна система захисту інформації – це сукупність заходів, процедур, технологій та політик, спрямованих на забезпечення конфіденційності, цілісності та доступності інформації в організації або системі. Основні складові такої системи включають:

1. Технічні заходи захисту: Це включає в себе застосування криптографічних методів, встановлення брандмауерів, антивірусного програмного забезпечення, систем виявлення вторгнень та інших технічних засобів для захисту мережі та систем.

2. Політики безпеки: Система повинна мати чітко визначені правила і політики щодо обробки, зберігання та передачі інформації, а також щодо доступу до неї. Це може включати політики паролів, рівні доступу, процедури аутентифікації та авторизації.

3. Фізичний захист: Заходи безпеки повинні охоплювати не лише цифрові аспекти, а й захист фізичного обладнання та приміщень, включаючи контроль доступу до серверних кімнат і обладнання.

4. Навчання та свідомість користувачів: Важливим аспектом є навчання персоналу щодо правил безпеки, ідентифікації загроз та способів запобігання атакам.

5. Аудит та моніторинг: Система повинна бути постійно аудитована та моніторингована для виявлення можливих порушень безпеки та інцидентів.

6. Резервне копіювання та відновлення: Наявність резервних копій даних та процедур відновлення є важливою складовою системи захисту інформації для забезпечення доступності та відновлення даних у випадку аварійних ситуацій чи атак. Ці компоненти спільно створюють комплексну систему захисту інформації, яка має захищати дані та інформаційні ресурси від різних загроз.