Назва навчальної дисципліни	**Комп'ютерна безпека**
Прізвище, ім'я, по батькові викладача	**Фурман О. А.**
Ти курсу	Вибіркова компонента
Рівень вищої освіти	Другий (магістерський)
Кількість кредитів/год	*4/120*
Науковий ступінь	*кандидат педагогічних наук*
Вчене звання	*доцент*
Посада викладача	*доцент кафедри інформаційних технологій та методики навчання*
Профайл викладача	http://www.kogpi.edu.te.ua/images/stories/Henrikh/teh_kaf/info_docs/Babij.pdf
E-mail викладача	*Ramskaoa@meta.ua*
Розклад консультацій	*Очні консультації*
Місце проведення	*48 ауд.*

Опис дисципліни

Предметом вивчення курсу Комп'ютерна безпека є інформаційне середовище Інтернету.

Об'єктом предмета Комп'ютерна безпека є способи доступу й використання *інформації*, наявної в *глобальній мережі.*

Комп'ютерну безпеку часто ототожнюють з поняттям *«кібербезпека».*

Завданнями вивчення дисципліни Комп'ютерна безпека є:

- вироблення навичок етичної роботи з *інформацією*;
- формування умінь критично оцінювати інформаційні матеріали, розміщені в мережі;
- зниження проявів піратства й плагіату в *глобальній мережі*;
- пропаганда в суспільстві поваги до інтелектуальної власності;
- гарантування прав особи на доступ до *інформації;*
- забезпечення розвитку *кібербезпеки* в Україні;
- вироблення умінь захищати програмні продукти від можливих мережевих атак.

Метою вивчення дисципліни Комп'ютерна безпека є формування у студентів умінь і навичок етичної та критичної роботи з інформацією, уміщеною в глобальній мережі, захисту власного інтелектуального надбання від несанкціонованого доступу та використання.

Політика дисципліни

Академічна доброчесність. Очікується, що роботи студентів будуть їх оригінальними дослідженнями чи міркуваннями. Відсутність посилань на використані джерела, фабрикування джерел, списування, втручання в роботу інших студентів становлять, але не обмежують, приклади можливої академічної недоброчесності. Виявлення ознак академічної недоброчесності в письмовій роботі студента є підставою для її незарахування викладачем, незалежно від масштабів плагіату.

Відвідування занять. Здобувачі вищої освіти зобов'язані: дотримуватися вимог законодавства, Статуту Академії; відвідувати усі види навчальних занять; складати (перескладати) залік; ліквідовувати академічну заборгованість у встановлені терміни.

Навчальний контент

.

Тема 1 Основні загрози та вразливості інформаційних систем.

Основні загрози та вразливості інформаційних систем включають в себе кібератаки, віруси, фішинг, витік конфіденційної інформації, несанкціонований доступ до даних, внутрішні загрози, а також недостатня кібербезпека та відсутність регулярного оновлення програмного забезпечення. Для запобігання цим загрозам необхідно вживати заходів з кібербезпеки, встановлювати антивірусне програмне забезпечення, навчати персоналу правилам безпеки та регулярно аудитувати інформаційну систему.

Тема 2. Принципи кібербезпеки та правила безпеки в IT.

Принципи кібербезпеки та правила безпеки в IT включають захист конфіденційності даних, використання сильних паролів, регулярне оновлення програмного забезпечення, використання антивірусного програмного забезпечення та обережне відкриття невідомих посилань чи вкладень в електронних листах.

Тема 3. Заходи забезпечення безпеки даних та інформації.

Забезпечення безпеки даних та інформації в сучасному цифровому світі є надзвичайно важливою задачею для організацій усіх масштабів. Для досягнення цього мети, слід вживати комплекс заходів, включаючи: **1.** Використання сильних паролів та механізмів двофакторної аутентифікації. **2.** Шифрування даних під час їх передачі та зберігання. **3.** Регулярне резервне копіювання інформації для запобігання втрат даних. **4.** Впровадження програм захисту від вірусів та інших шкідливих програм. **5.** Обмін інформацією лише по захищених каналах зв'язку. **6.** Навчання персоналу правилам кібербезпеки та практикам безпеки даних.

Тема 4. Криптографічні методи захисту інформації.

Симетричне шифрування – використовує один ключ для шифрування і дешифрування (AES, DES).

Асиметричне шифрування – використовує пару ключів: публічний для шифрування і приватний для дешифрування (RSA, ElGamal).

Хешування – перетворює дані в хеш для перевірки цілісності (SHA, MD5).

Цифровий підпис – підтверджує справжність і цілісність даних.

Стеганографія – приховує сам факт передачі інформації, вбудовуючи її в інші дані.

Тема 5. **Захист від мережевих загроз: віруси, хакери, фішинг.**

Віруси – шкідливі програми, що поширюються через файли та виконують деструктивні дії на пристроях. Захист: антивіруси, регулярні оновлення.

Хакери – зловмисники, що зламують системи для крадіжки даних або отримання доступу. Захист: брандмауери, двофакторна аутентифікація, сильні паролі.

Фішинг – шахрайські спроби отримати конфіденційну інформацію через підроблені сайти або електронні листи. Захист: навчання користувачів, антифішингові інструменти, уважність до підозрілих повідомлень.

Тема 6. **Законодавство у сфері кібербезпеки**

Захист персональних даних – закони, що регулюють обробку та зберігання особистої інформації (наприклад, GDPR у ЄС).

Кіберзлочини – кримінальна відповідальність за несанкціоновані доступи, зломи систем і крадіжку даних.

Захист критичної інфраструктури – правила для захисту важливих для держави систем (енергетика, транспорт).

Міжнародне співробітництво – угоди між країнами для спільної боротьби з кіберзагрозами.

Методи навчання
Лабораторні роботи, пояснення, розповідь, демонстрація.
Методи контролю
Опитування, ІНДЗ, самостійна робота, залік

Політика оцінювання : заняття проводяться у формі дискусій, мозкових штурмів; висловлювання власної точки зору заохочується; нетерпимість до академічного плагіату. На лекційних заняттях проводяться бліц-опитування щодо аналізу останніх новин галузі рекламно-інформаційних технологій та результативності роботи на сучасному етапі. Оцінюються актуальна новина, ґрунтовне пояснення і власна точка зору.

Інформаційне забезпечення

1. Комп'ютерна безпека // Захист інформації в комп'ютерних системах: підручник [Архівовано 21 Січня 2022 у Wayback Machine.] / Козюра В. Д., Хорошко В. О., Шелест М. Є., Ткач Ю. М., Балюнов О. О. — Ніжин: ФОП Лук'яненко В. В., ТПК «Орхідея», 2020. — 12. — 236 с. — ISBN 978-617-7609-44-4.

2. ↑ Закон України «Про основні засади забезпечення кібербезпеки України» від 5 жовтня 2017 року № 2163-VIII. Архів оригіналу за 13 Листопада 2017. Процитовано 13 Листопада 2017.

3. ↑ Кібербезпека чи Інформаційна безпека? | Блоги | Компьютерное Обозрение. ko.com.ua (ukr) . Архів оригіналу за 3 Червня 2019. Процитовано 3 червня 2019. {{cite web}}: |first= з пропущеним |last= (довідка)

4. ↑ A General Framework for Formal Notions of «Secure» Systems [Архівовано 8 Березня 2012 у Wayback Machine.] — B. Pfitzmann, M. Waidner, Hildesheimer Informatik-Berichte

Інформаційні ресурси

1. mangustfilms/index.php?newsid=993
2. litsovet/
3. rigamedia.com
4. videocifra

1.