

**МІНІСТЕРСТВО ВНУТРІШНІХ СПРАВ УКРАЇНИ
ХАРКІВСЬКИЙ НАЦІОНАЛЬНИЙ УНІВЕРСИТЕТ
ВНУТРІШНІХ СПРАВ**

Кафедра протидії кіберзлочинності факультету №4

**МЕТОДИЧНІ МАТЕРІАЛИ
ДО СЕМІНАРСЬКИХ ЗАНЯТЬ**

з навчальної дисципліни "Інформаційно-комунікаційні системи у протидії
злочинам, пов'язаним з торгівлею людьми"
вибіркових компонент
освітньої програми першого рівня вищої освіти

262 Правоохоронна діяльність (Протидія торгівлі людьми)

ЗАТВЕРДЖЕНО

Науково-методичною радою
Харківського національного
університету внутрішніх справ
Протокол від 29.01.2024 № 1

СХВАЛЕНО

Вченою радою факультету №4
Протокол від 17.01.2024 № 1

ПОГОДЖЕНО

Секцією науково-методичної ради
ХНУВС з технічних дисциплін
Протокол від 26.01.2024 № 1

Розглянуто на засіданні кафедри протидії кіберзлочинності (протокол № 1 від 10.01.2024

Розробник: старший викладач кафедри протидії кіберзлочинності ХНУВС, підполковник поліції Грищенко Д.О.

Рецензенти:

доцент кафедри кібербезпеки та DATA-технологій факультету №6 Харківського національного університету внутрішніх справ к.т.н. доцент Тулупов В.В.

перший проректор Харківського університету, д.ю.н., професор Павликівський В.І.

1. Розподіл часу навчальної дисципліни за темами

Номер та назва навчальної теми	Кількість годин відведених на вивчення навчальної дисципліни					Вид контролю
	Всього	з них:				
		лекції	Семінарські заняття	Практичні заняття	Самостійна робота	
Семестр №4						
Тема №1. Соціальна інженерія	13	2	2		8	залік
Тема №2. Безпечне користування мережею Інтернет	13	2	2	2	8	
Тема №3. Безпечне користування електронною поштою	12	2	2	2	8	
Тема №4. Шкідливе програмне забезпечення	14	1	2	2	10	
Тема №5. Безпека користування соціальними мережами	14	1	2		10	
Тема №6. Безпека мобільних пристроїв	12	1		2	8	
Тема №7. Фізична безпека	12	1		2	8	
Всього за дисципліною	90	10	10	10	60	

2. Методичні вказівки до семінарських занять

Тема №1. Соціальна інженерія

Семінарське заняття 1.1. Соціальна інженерія

Навчальна мета заняття: обговорити та засвоїти поняття, методи та послідовність атаки із використанням соціальної інженерії

Кількість годин: 2 год.

Навчальні питання

1. Поняття соціальної інженерії.
2. Методи соціальної інженерії.
3. Етапи атаки із використанням соціальної інженерії.

Література: [2, с. 8 – 40]

План проведення заняття

1. Поняття соціальної інженерії.

Заслухати цільовий виступ здобувача із рефератом за темою "Огляд актуальних атак із використанням соціальної інженерії".

Обговорити природу і причин успішності атак із використанням соціальної інженерії.

2. Методи соціальної інженерії.

Запропонувати здобувачам провести класифікацію методів соціальної інженерії за різними ознаками.

3. Етапи атаки із використанням соціальної інженерії.

Обговорити етапи атаки із використанням соціальної інженерії та зазначити актуальні засоби їх проведення.

Виставити оцінки. Зазначити перелік задач для самостійної роботи, вказати час і спосіб перевірки результатів самостійної роботи.

Оголосити тему наступного заняття.

Тема №2. Безпечне користування мережею Інтернет

Семінарське заняття 2.1. Безпечне користування мережею Інтернет

Навчальна мета заняття: обговорити та засвоїти рекомендації із безпечного користування мережею Інтернет

Кількість годин: 2 год.

Навчальні питання

1. Безпека браузерів.
2. Безпека даних.

Література: [2, с. 41 – 51]

План проведення заняття

1. Безпека браузерів.

Заслухати цільовий виступ здобувача із рефератом за темою "Кібератаки з використанням інтернет-браузеру".

Обговорити технології, що забезпечують роботу браузеру, та безпечність його використання.

2. Безпека даних.

Обговорити убезпечення даних при користуванні Wi-Fi мереж.

Виставити оцінки. Зазначити перелік задач для самостійної роботи, вказати час і спосіб перевірки результатів самостійної роботи.

Оголосити тему наступного заняття.

Тема №3. Безпечне користування електронною поштою

Семінарське заняття 3.1. Безпечне користування електронною поштою

Навчальна мета заняття: обговорити та засвоїти рекомендації із безпечного користування електронною поштою

Кількість годин: 2 год.

Навчальні питання

1. Кібератаки через електронну пошту.
2. Убезпечення поштового облікового запису.

Література: [2, с. 55 – 69]

План проведення заняття

1. Кібератаки через електронну пошту.

Заслухати цільовий виступ здобувача із рефератом за темою "Кібератаки через електронну пошту".

Обговорити як відрізнити легітимні листи від фішингових.

2. Убезпечення поштового облікового запису.

Обговорити рекомендації убезпечення поштового облікового запису.

Виставити оцінки. Зазначити перелік задач для самостійної роботи, вказати час і спосіб перевірки результатів самостійної роботи.

Оголосити тему наступного заняття.

Тема №4. Шкідливе програмне забезпечення

Семінарське заняття 4.1. Шкідливе програмне забезпечення

Навчальна мета заняття: обговорити шляхи розповсюдження і засвоїти дії при ураженні шкідливим програмним забезпеченням

Кількість годин: 2 год.

Навчальні питання

1. Шляхи розповсюдження ШПЗ, вектори атак.
2. Дії при ураженні шкідливим програмним забезпеченням.

Література: [2, с. 69 – 95]

План проведення заняття

1. Шляхи розповсюдження ШПЗ, вектори атак.

Заслухати цільовий виступ здобувача із рефератом за темою "Шляхи розповсюдження шкідливого програмного забезпечення".

Обговорити види шкідливого програмного забезпечення.

2. Ознаки ураження шкідливим програмним забезпеченням.

Обговорити дії при ураженні шкідливим програмним забезпеченням.

Виставити оцінки. Зазначити перелік задач для самостійної роботи, вказати час і спосіб перевірки результатів самостійної роботи.

Оголосити тему наступного заняття.

Тема №5. Безпека користування соціальними мережами

Семінарське заняття 5.1. Безпека користування соціальними мережами

Навчальна мета заняття: обговорити і засвоїти рекомендації із безпечного користування соціальними мережами.

Кількість годин: 2 год.

Навчальні питання

1. Реєстрація у соцмережах.

2. Рекомендації із безпечного користування соціальними мережами.

Література: [2, с. 97 – 103]

План проведення заняття

1. Реєстрація у соцмережах.

Заслухати цільовий виступ здобувача із рефератом за темою "Загрози при користуванні соціальними мережами".

Обговорити безпечну реєстрацію у соцмережах.

2. Рекомендації із безпечного користування соціальними мережами.

Обговорити рекомендації із безпечного користування соціальними мережами.

Виставити оцінки. Зазначити перелік задач для самостійної роботи, вказати час і спосіб перевірки результатів самостійної роботи.

Оголосити тему наступного заняття.

3. Рекомендована література (основна, допоміжна), інформаційні ресурси в Інтернеті

Основна

1. Манжай О., Носов В. Методичний посібник для тренерів з питань кібергігієни у рамках спеціальної професійної (сертифікатної) програми підвищення кваліфікації: Практикум. Київ: ВАІТЕ, 2021.-106 с.
2. Робочий зошит для учасників тренінгу з питань кібергігієни. Загальна короткострокова програма підвищення кваліфікації. // Барановський Олексій, Гузій Василь, Майорников Демид, Манжай Олександр, Носов Віталій. – Київ: ВАІТЕ, 2021. – 262 с.

Допоміжна

3. Security Tip (ST04-014). Avoiding Social Engineering and Phishing Attacks. URL: <https://us-cert.cisa.gov/ncas/tips/ST04-014>. Original release date: October 22, 2009 | Last revised: August 25, 2020.
4. Social Engineering: The Art of Human Hacking – Christopher Hadnagy, ISBN: 978-0-470-63953-5 December 2010.

Інформаційні ресурси

5. <https://osvita.diia.gov.ua/courses/cyber-hygiene>