МІНІСТЕРСТВО ВНУТРІШНІХ СПРАВ УКРАЇНИ

ХАРКІВСЬКИЙ НАЦІОНАЛЬНИЙ УНІВЕРСИТЕТ ВНУТРІШНІХ СПРАВ

Кафедра протидії кіберзлочинності факультету №4

РОБОЧА ПРОГРАМА

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)

Харків 2024

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. Опис навчальної дисципліни

Найменування показників	Шифри та назви галузі знань, код та назва спеціальності, ступінь вищої освіти	Характеристика навчальної дисципліни
Кількість кредитів ECTS – 3 Загальна кількість годин – 90 Кількість тем – 7	26 Цивільна безпека 262 Правоохоронна діяльність (Протидія торгівлі людьми) бакалавр	Навчальний курс 2 Семестри 4 Види підсумкового контролю: залік

Розподіл навчальної дисципліни за видами занять:	
денна форма навчання	заочна форма навчання
Семестр 4: Лекції – 10 год; Семінарські заняття - 10 год; Практичні заняття – 10 год; Самостійна робота – 60 год; Індивідуальні завдання: Реферати (тощо) – 1	Лекції – 8 год; Семінарські заняття - 10 год; Самостійна робота – 72 год; Індивідуальні завдання: Реферати (тощо) – 1

2. Мета та завдання навчальної дисципліни

Метою викладання навчальної дисципліни "Інформаційно-комунікаційні системи у протидії злочинам, пов'язаним з торгівлею людьми" є формування знань і вмінь безпечно використовувати інформаційно-комунікаційні системи у протидії злочинам, пов'язаним з торгівлею людьми.

Основними завданнями вивчення дисципліни "Інформаційно-комунікаційні системи у протидії злочинам, пов'язаним з торгівлею людьми" є:

- ознайомлення із основними кіберзагрозами для ресурсів інформаційно-комунікаційних систем і способами захисту від них;
- формування навичок безпечно використовувати інформаційно-комунікаційні системи у протидії злочинам, пов'язаним з торгівлею людьми.

Згідно з освітньою програмою здобувачі вищої освіти повинні:

знати: основні кіберзагрози для ресурсів інформаційно-комунікаційних систем і способи захисту від них;

вміти: безпечно використовувати інформаційно-комунікаційні системи у протидії злочинам, пов'язаним з торгівлею людьми.

Програмні компетентності, які формуються при вивченні навчальної дисципліни:		
Інтегральна компетентність	Здатність вирішувати складні спеціалізовані задачі та практичні проблеми у сфері правоохоронної діяльності або у процесі навчання, що передбачає застосування певних теорій та методів правоохоронної діяльності і характеризується комплексністю та невизначеністю умов.	
Загальні компетентності (ЗК)	ЗК 1	Здатність застосовувати знання у практичних ситуаціях.
	ЗК 4	Здатність використовувати інформаційні комунікаційні технології.
Спеціальні (фахові, предметні) компетентності	СК 18	Здатність забезпечувати кібербезпеку, економічну та інформаційну безпеку держави, об’єктів критичної інфраструктури.

3. Програма навчальної дисципліни

Тема №1. Соціальна інженерія

Поняття соціальної інженерії. Причини та умови соціальної інженерії. Прийоми, методи та принципи соціальної інженерії. Психологія впливу та загальні рекомендації для органів публічної влади.

Тема №2. Безпечне користування мережею Інтернет

Браузер та його функції. Доменні імена. Шифрування комунікацій. Організація авторизації в Інтернеті з використанням браузера. Безпечне використання плагінів. Рекомендації з убезпечення браузеру. Безпечне користування мережами Wi-Fi. Відповідальне оприлюднення інформації.

Тема №3. Безпечне користування електронною поштою

Розмежування використання особистої та службової поштових скриньок. Загрози під час користування поштовою скринькою. Аналіз листів, що містять ознаки фішингу. Рекомендації щодо захисту електронної пошти. План дій на випадок компрометації пошти.

Тема №4. Шкідливе програмне забезпечення

Загрози для програмного забезпечення. Оновлення програмного забезпечення. Ліцензійне та неліцензійне програмне забезпечення. Типи шкідливого програмного забезпечення. План дій у випадку зараження інформаційної системи. Загальні рекомендації з використання програмного забезпечення.

Тема №5. Безпека користування соціальними мережами

Соціальні мережі: загальні положення. Безпечна реєстрація в соціальних мережах. Налаштування конфіденційності та інших питань безпеки. Шахрайство в соціальних мережах. Відповідальне розповсюдження інформації у соціальних мережах. Рекомендації з безпечної роботи в соціальних мережах.

Тема №6. Безпека мобільних пристроїв

Правила обмеження доступу до мобільних пристроїв. Безпечна робота в мультимедійних засобах спілкування. Особливості передавання вживаних мобільних пристроїв іншим особам. Особливості передавання контактної інформації іншим особам. Головні загрози, які виникають під час роботи з мобільними пристроями. Основні правила безпечної роботи з мобільними пристроями.

Тема №7. Фізична безпека

Роль фізичної безпеки у кіберзахисті організації. Безпека контрольованої зони. Загрози, які виникають під час використання змінних носії інформації. Рекомендації щодо фізичної безпеки.

4. Структура навчальної дисципліни

4.1.1. Розподіл часу навчальної дисципліни за темами (денна форма навчання)

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	
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	**залік**
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**	

4.1.2. Питання, що виносяться на самостійне опрацювання

Перелік питань до тем навчальної дисципліни	Література
Тема №1. Соціальна інженерія	
Відпрацювати лекцію за темою. Підготувати виступ на семінарі	1,2,5, ресурси Internet
Тема №2. Безпечне користування мережею Інтернет	
Відпрацювати лекцію за темою. Підготувати виступ на семінарі Закінчити виконання практичного заняття та надати звіт	1,2,5, ресурси Internet
Тема №3. Безпечне користування електронною поштою	
Відпрацювати лекцію за темою. Підготувати виступ на семінарі Закінчити виконання практичного заняття та надати звіт	1,2,5, ресурси Internet
Тема №4. Шкідливе програмне забезпечення	
Відпрацювати лекцію за темою. Підготувати виступ на семінарі Закінчити виконання практичного заняття та надати звіт	1,2,5, ресурси Internet
Тема №5. Безпека користування соціальними мережами	
Відпрацювати лекцію за темою. Закінчити виконання практичного заняття та надати звіт	1,2,5, ресурси Internet
Тема №6. Безпека мобільних пристроїв	
Відпрацювати лекцію за темою. Підготувати виступ на семінарі	1,2,5, ресурси Internet
Тема №7. Фізична безпека	
Відпрацювати лекцію за темою. Закінчити виконання практичного заняття та надати звіт	1,2,5, ресурси Internet

5. Індивідуальні навчально-дослідні завдання

5.1.1. Теми рефератів

1. Порівняльний аналіз технологій соціальної інженерії.
2. Технології TOR мережі.
3. Технології I2P мережі.
4. Порівняльний аналіз безкоштовних персональних міжмережних екранів.
5. Аналіз сучасних тенденцій шкідливого програмного забезпечення.
6. Порівняльний аналіз безпечності мобільних месенджерів.

6. Методи навчання

Аудиторні заняття проводяться у формі візуального представлення аналітично-графічного матеріалу дисципліни, на яких курсанти повинні виконувати відповідні розумові, обчислювальні та практичні дії.

Самостійна робота за кожною темою передбачає вивчення теоретичних питань лекційних занять, опрацювання завдань семінарських і практичних занять.

Індивідуальна робота передбачає написання рефератів.

7. Перелік питань та завдань, що виносяться на підсумковий контроль

1. Поняття соціальної інженерії.
2. Причини та умови соціальної інженерії.
3. Прийоми, методи та принципи соціальної інженерії.
4. Психологія впливу та загальні рекомендації для органів публічної влади.
5. Браузер та його функції.
6. Доменні імена.
7. Шифрування комунікацій.
8. Організація авторизації в Інтернеті з використанням браузера.
9. Безпечне використання плагінів.
10. Рекомендації з убезпечення браузеру.
11. Безпечне користування мережами Wi-Fi.
12. Відповідальне оприлюднення інформації.
13. Розмежування використання особистої та службової поштових скриньок.
14. Загрози під час користування поштовою скринькою.
15. Аналіз листів, що містять ознаки фішингу.
16. Рекомендації щодо захисту електронної пошти.
17. План дій на випадок компрометації пошти.
18. Загрози для програмного забезпечення.
19. Оновлення програмного забезпечення.
20. Ліцензійне та неліцензійне програмне забезпечення.
21. Типи шкідливого програмного забезпечення.
22. План дій у випадку зараження інформаційної системи.
23. Загальні рекомендації з використання програмного забезпечення.
24. Соціальні мережі: загальні положення.
25. Безпечна реєстрація в соціальних мережах.
26. Налаштування конфіденційності та інших питань безпеки.
27. Шахрайство в соціальних мережах.
28. Відповідальне розповсюдження інформації у соціальних мережах.
29. Рекомендації з безпечної роботи в соціальних мережах.
30. Правила обмеження доступу до мобільних пристроїв.
31. Безпечна робота в мультимедійних засобах спілкування.
32. Особливості передавання вживаних мобільних пристроїв іншим особам.
33. Особливості передавання контактної інформації іншим особам.
34. Головні загрози, які виникають під час роботи з мобільними пристроями.
35. Основні правила безпечної роботи з мобільними пристроями.
36. Роль фізичної безпеки у кіберзахисті організації.
37. Безпека контрольованої зони.
38. Загрози, які виникають під час використання змінних носії інформації.
39. Рекомендації щодо фізичної безпеки.

8. Критерії та засоби оцінювання результатів навчання здобувачів

Контрольні заходи включають у себе поточний та підсумковий контроль.

Поточний контроль.

До форм поточного контролю належить оцінювання:

- рівня знань під час практичних і семінарських занять;
- якості виконання індивідуальної та самостійної роботи.

Поточний контроль здійснюється під час проведення практичних та семінарських занять і має за мету перевірку засвоєння знань, умінь і навичок здобувачем вищої освіти (далі – здобувач) з навчальної дисципліни.

У ході поточного контролю проводиться систематичний вимір приросту знань, їх корекція. Результати поточного контролю заносяться викладачем до журналів обліку роботи академічної групи за національної системою оцінювання («відмінно», «добре», «задовільно», «незадовільно»).

Оцінки за самостійну та індивідуальну роботи виставляються в журнали обліку роботи академічної групи окремою графою за національною системою оцінювання («відмінно», «добре», «задовільно», «незадовільно»). Результати цієї роботи враховуються під час виставлення підсумкових оцінок.

При розрахунку успішності здобувачів враховуються такі види робіт: навчальні заняття (практичні, лабораторні тощо); самостійна та індивідуальна роботи (виконання домашніх завдань, ведення конспектів першоджерел та робочих зошитів, виконання розрахункових завдань, підготовка рефератів, наукових робіт, публікацій, розроблення спеціальних технічних пристроїв і приладів, моделей, комп'ютерних програм, виступи на наукових конференціях, семінарах та інше); контрольні роботи (виконання тестів, контрольних робіт у вигляді, передбаченому в робочій програмі навчальної дисципліни). Вони оцінюються за національною системою оцінювання («відмінно», «добре», «задовільно», «незадовільно»).

Здобувач, який отримав оцінку «незадовільно» за навчальні заняття або самостійну роботу, зобов'язаний перескласти її.

Загальна кількість балів (оцінка), отримана здобувачем за семестр перед підсумковим контролем, розраховується як середньоарифметичне значення з оцінок за навчальні заняття та самостійну роботу, та для переводу до 100-бальної системи помножується на коефіцієнт **10**.

Загальна кількість балів (перед підсумковим контролем) ***=((Результат навчальних занять за семестр + Результат самостійної роботи за семестр) / 2) *10***

Підсумковий контроль. Підсумковий контроль проводиться з метою оцінки результатів навчання на певному ступені вищої освіти або на окремих його завершених етапах.

Для обліку результатів підсумкового контролю використовується поточно-накопичувальна інформація, яка реєструються в журналах обліку роботи академічної групи. Результати підсумкового контролю з дисциплін відображуються у відомостях обліку успішності, навчальних картках здобувачів, залікових книжках. ***Присутність здобувачів на проведенні підсумкового контролю (заліку, екзамену) обов'язкова.*** Якщо здобувач вищої освіти не з'явився на підсумковий контроль (залік, екзамен), то науково-педагогічний працівник ставить у відомість обліку успішності відмітку «не з'явився».

Підсумковий контроль (екзамен, залік) оцінюється за національною шкалою. Для переводу результатів, набраних на підсумковому контролі, з національної системи оцінювання в 100-бальну вводиться коефіцієнт **10**, таким чином максимальна кількість балів на підсумковому контролі (екзамені, заліку), які використовуються при розрахунку успішності здобувачів, становить **50.**

Підсумкові бали з навчальної дисципліни визначаються як сума балів, отриманих здобувачем протягом семестру, та балів, набраних на підсумковому контролі (екзамені, заліку).

Підсумкові бали навчальної дисципліни = ***Загальна кількість балів (перед підсумковим контролем)*** + ***Кількість балів за підсумковим контролем***

Здобувач вищої освіти, який під час складання підсумкового контролю (екзамен, залік) отримав незадовільну оцінку, складає його повторно. Повторне складання підсумкового екзамену чи заліку допускається не більше двох разів з кожної навчальної дисципліни: один раз – викладачеві, а другий – комісії, до складу якої входить керівник відповідної кафедри та 2-3 науково-педагогічних працівники.

Якщо дисципліна вивчається протягом двох і більше семестрів з семестровим контролем у формі екзамену чи заліку, то результат вивчення дисципліни в поточному семестрі визначається як середньоарифметичне значення балів, набраних у поточному та попередньому семестрах.

Підсумкові бали навчальної дисципліни = ***Підсумкові бали за поточний семестр*** + ***Підсумкові бали за попередній семестр*** : ***2***

Критерії оцінювання здобувачів вищої освіти під час поточного контролю *(робота на практичних, лабораторних заняттях, самостійна робота, виконання індивідуальних творчих завдань)* та підсумкового контролю.

Робота під час навчальних занять	**Самостійна та індивідуальна робота**	**Підсумковий контроль**
Отримати не менше 4 позитивних оцінок	Підготувати реферат, підготувати звіт за темою самостійної роботи.	Отримати за підсумковий контроль не менше 30 балів

9. Шкала оцінювання: національна та ECTS

Оцінка в балах		Оцінка за національною шкалою	Оцінка за шкалою ECTS	
			Оцінка	Пояснення
12	97–100	Відмінно ("зараховано")	A	**"Відмінно"** – теоретичний зміст курсу освоєний **цілком,** необхідні практичні навички роботи з освоєним матеріалом сформовані, **всі** навчальні завдання, які передбачені програмою навчання **виконані** в повному обсязі, відмінна робота без помилок або з однією незначною помилкою.
11	94-96			
10	90-93			
9	85– 89	Добре ("зараховано")	B	**"Дуже добре"** – теоретичний зміст курсу освоєний **цілком**, необхідні практичні навички роботи з освоєним матеріалом **в основному** сформовані, **всі** навчальні завдання, які передбачені програмою навчання **виконані**, якість виконання **більшості** з них оцінено числом балів, близьким до **максимального,** робота з двома – трьома незначними помилками.
8	80-84			
7	75–79		C	**"Добре"** – теоретичний зміст курсу освоєний **цілком**, практичні навички роботи з освоєним матеріалом **в основному** сформовані, **всі** навчальні завдання, які передбачені програмою навчання **виконані**, якість виконання **жодного** з них **не оцінено мінімальним** числом балів, деякі види завдань виконані **з помилками,** робота з декількома незначними помилками, або з однією – двома значними помилками.
6	70 –74	Задовільно ("зараховано")	D	**"Задовільно"** – теоретичний зміст курсу освоєний **не повністю**, але **прогалини не носять істотного** характеру, необхідні практичні навички роботи з освоєним матеріалом **в основному** сформовані, **більшість** передбачених програмою навчання навчальних завдань **виконано, деякі** з виконаних завдань, містять **помилки,** робота з трьома значними помилками.
5	65-69			
4	60–64		E	**"Достатньо"** – теоретичний зміст курсу освоєний **частково, деякі** практичні навички роботи **не сформовані, частина** передбачених програмою навчання навчальних завдань **не виконані,** або якість виконання деяких з них оцінено числом балів, близьким до **мінімального**, робота, що задовольняє мінімуму критеріїв оцінки.
3	41–59	Незадовільно ("не зараховано")	FX	**"Умовно незадовільно"** – теоретичний зміст курсу освоєний **частково**, необхідні практичні навички роботи **не сформовані, більшість** передбачених програм навчання, навчальних завдань **не виконано**, або якість їхнього виконання оцінено числом балів, близьким до **мінімального**; при **додатковій самостійній** роботі над матеріалом курсу **можливе підвищення якості** виконання навчальних завдань (**з можливістю повторного складання**), робота, що потребує доробки
2	21-40			
1	1–20		F	**"Безумовно незадовільно"** – теоретичний зміст курсу **не освоєно**, необхідні практичні навички роботи **не**

Оцінка в балах		Оцінка за національною шкалою	Оцінка за шкалою ECTS	
			Оцінка	Пояснення
				сформовані, всі виконані навчальні завдання містять грубі **помилки, додаткова самостійна** робота над матеріалом курсу **не приведе** до значимого **підвищення якості** виконання навчальних завдань, робота, що потребує повної переробки

10. 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