МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ
КИЇВСЬКИЙ НАЦІОНАЛЬНИЙ ЕКОНОМІЧНИЙ
УНІВЕРСИТЕТ імені Вадима Гетьмана

ІНСТИТУТ ПІСЛЯДИПЛОМНОЇ ОСВІТИ

«ЗАТВЕРДЖЕНО»
Вченою радою ДВНЗ "Київський національний економічний університет імені Вадима Гетьмана "
(протокол № ___від_25 лютого__2021 р.)

Голова вченої ради ДВНЗ ”Київський національний економічний університет імені Вадима Гетьмана ”

_____Д.Г. Лук’яненко

НАВЧАЛЬНИЙ ПЛАН

курсів підвищення кваліфікації
науково-педагогічних та педагогічних працівників
закладів вищої та фахової передвищої освіти

«Інструменти аналізу кіберзлочинів та цифрова гігієна»

Термін навчання — 8 тижнів, 120 год.

форма навчання — без відриву від виробництва

Науковий керівник:
д.ф.м.н., проф. Джалладова І.А.,
зав. кафедрою комп’ютерної математики
та інформаційної безпеки КНЕУ

Науково-педагогічні працівники, що забезпечують навчання:
д.ф.м.н., проф. Джалладова І.А.,
д.т.н., проф. Толюпа С.В.,
к.е.н., проф. Бєгун А.В.,
ст.викл. Урденко О.Г.

Київ—2021

Найменування розділів	*години*				
	усього	*у тому числі*			
		теоретична підготовка (лекції)	*тренінг*	*робота в дистанційному режимі*	*самостійна робота*
1	2	3	4	5	6
***Модуль І.* Цифрова гігієна інформаційних технологій та засоби її дотримання (для початківців)**					
1.1. Кібербезпека як частина кібергігієни та інтернет-гігієни.	2	2			
1.2. Цифровий відбиток та цифрова гігієна як елементи цифрової особистості.	1	1			
1.3. Активні та пасивні цифрові відбитки (сліди).	2	1	1		
1.4. Ризики інформаційної безпеки у онлайнових комунікаціях у соціальних мережах.	2	1	1		
1.5. Кореляційний аналіз безпеки та конфіденційності.	2	1	1		
1.6. Захист даних як елемент цифрової гігієни.	1	1			
1.7. Закони і практичні методи, які забезпечують захист персональних даних в різних країнах світу.	3	2	1		
1.8. Способи поширення шкідливого ПЗ в інтернет для впливу шкідливого ПЗ на систему користувача.	3	2	1		
1.9. Безпека авторських прав на інтелектуальні твори в інтернеті: ігри, програмне забезпечення, музика, фільми, файли, поштові повідомлення.	3	2	1		
1.10. Кіберзлочини проти особистості: економічні наслідки для жертв, втрати соціального статусу і репутаційна шкода.	3	2	1		
1.11. Цифрова гігієна робочого місця, практичні методи аналізу та зачищення цифрових слідів у комп'ютерних системах (контркриміналістика) від наслідків інтернет-серфінгу з використанням спеціальних програмних засобів.	4	2	2		
1.12. Впорядковані данні поштових скриньок. Поштові клієнти	3	2	1		
1.13. Використання безпечних паролів, диспетчер паролів.	2	1	1		
1.14. Налаштування конфіденційності та безпеки в акаунтах і соціальних мережах	3	2	1		
1.15. Контрольне тестування.	2		2		
Усього за модулем І	**36**	**22**	**14**		

Найменування розділів	*години*				
	усього	*у тому числі*			
		теоретична підготовка (лекції)	*тренінг*	*робота в дистанційному режимі*	*самостійна робота*
1	2	3	4	5	6
***Модуль ІІ*. Цифрова криміналістика (для продвинутих користувачів)**					
1.1. Про кіберзлочинність.	1	1			
1.2. Джерела кіберзлочинності, основні види.	1	1			
1.3. Стандарти та нормативно-правові акти інформаційної безпеки.	2	1	1		
1.4. Зв'язок стандартів та сучасних практичних методів дослідження в області цифрової криміналістики.	2	1	1		
1.5. Кореляційний аналіз безпеки та конфіденційності.	1	1			
1.6. Особливості кіберзлочинів в сфері інтелектуальної власності.	1	1			
1.7. Безпека авторських прав творів в інтернеті: ігри, програмне забезпечення, музика, фільми, файли, електрона пошта.	2	1	1		
1.8. Особливості стану конфіденційності та захисту персональних даних.	2	1	1		
1.9. Хактівізм, тероризм, шпигунство, дезінформаційні кампанії та війни в кіберпросторі.	3	2	1		
1.10. Кіберзлочини проти особистості: економічні наслідки для жертв, втрати соціального статусу і репутаційна шкода.	3	2	1		
1.11. Економічна та юридична оцінка економічних збитків від слідів і наслідків доступу до цифрових пристроїв.	2	1	1		
1.12. Інциденти інформаційної безпеки, розслідування кіберзлочинів.	3	2	1		
1.13. Цифрова криміналістика	2	1	1		
1.14. Цифрова криміналістика мережі, бездротових мереж, баз даних, електронної пошти, пам'яті.	3	2	1		
1.15. Основи комп'ютерно-технічної (цифрової) судової експертизи	2	2			
1.16. Основні концепції та методологія збору доказів за допомоги цифрової криміналістики	3	2	1		
1.17. Типи об’єктів цифрової криміналістики	2	2			
1.18. Загальні відомості про збір даних	1	1			
1.19. Концепції збору і дублювання даних	2	1	1		
1.20. Типи систем збору даних.	2	1	1		

Найменування розділів	*години*				
	усього	*у тому числі*			
		теоретична підготовка (лекції)	*тренінг*	*робота в дистанційному режимі*	*самостійна робота*
1	2	3	4	5	6
1.21. Спеціалізоване програмне забезпечення для цифрової криміналістики .	4	2	2		
1.22. Базові методи використання спеціалізованого програмного забезпечення для цифрової криміналістики.	4	2	2		
1.23. Дослідження жорстких дисків (HDD), твердотільних накопичувачів (SSD) і файлових систем.	3	2	1		
1.24. Цифрова криміналістична експертиза ОС Windows.	2	1	1		
1.25. Цифрова криміналістична експертиза енерго залежних даних ОС.	3	2	1		
1.26. Цифрова криміналістична експертиза мережі, логи і дампи мережевого трафіку	3	2	1		
1.27. Цифрова криміналістична експертиза веб-сайтів.	3	2	1		
1.28. Цифрова криміналістична експертиза систем управління базами даних (СУБД)	3	2	1		
1.29. Цифрова криміналістична експертиза хмарних технологій	3	2	1		
1.30. Цифрова криміналістична експертиза дій шкідливого програмного забезпечення	3	2	1		
1.31. Цифрова криміналістична експертиза електронної пошти	2	1	1		
1.32. Цифрова криміналістична експертиза мобільних пристроїв	3	2	1		
1.33. Техніки контркриміналістики - цифрова гігієна	3	2	1		
1.34. Важливі аспеки підготовка звіту про дослідження цифрових об’єктів.	3	2	1		
1.35. Контрольне тестування.	2	2			
Усього за модулем ІІ	**84**	**55**	**29**		
Разом	**120**	**77**	**43**		

Завідувач кафедри
комп’ютерної математики
та інформаційної безпеки І. А. Джалладова

Директор Інституту післядипломної освіти Д.В. Гризоглазов