Інформаційний пакет освітніх компонент навчального плану
освітньо-професійної програми Інформаційна та кібернетична безпека
(назва)

Освітнього рівня **першого (бакалаврського) рівня вищої освіти**

Спеціальності **125 «Кібербезпека»**

Галузь знань **12 «Інформаційні технології»**

1. Назва освітньої компоненти **Цифрова криміналістика**
(назва дисципліни)

2. Тип основна, вибіркова (вказати) вибіркова

3. Обсяг:	Кредитів ECTS	Годин	За видами занять:				
			Лекцій	Семінар	Практичних занять	Лабораторних занять	Самостійна підготовка
	5	150	18		18	18	96
4. Взаємозв'язок у структурно-логічній схемі							
Освітні компоненти, які передують вивченню	1. Комп'ютерні мережі 2. Теоретичні основи захищених інформаційно-комунікаційних технологій 3. Аналіз та оцінка уразливостей інформаційних систем 4. Основи захисту конфіденційних даних 5. Безпека безпроводових, мобільних та хмарних технологій 6. Аудит систем захисту інформації						
Освітні компоненти для яких є базовою	1. Переддипломна практика 2. Бакалаврська робота						
5. Компетенції відповідно до ОПП та вимог роботодавців:							
Компетенції відповідно до ООП							
Знати			**Вміти**				
ЗК 2. Знання та розуміння предметної області та розуміння професії.			ЗК 1. Здатність застосовувати знання у практичних ситуаціях.				
			ЗК 5. Здатність до пошуку, оброблення та аналізу інформації.				
			ЗК 7. Здатність зберігати та примножувати моральні, культурні, наукові цінності і досягнення суспільства на основі розуміння історії та				

	закономірностей розвитку предметної області, її місця у загальній системі знань про природу і суспільство та у у розвитку суспільства, техніки і технологій, використовувати різні види та форми рухової активності для активного відпочинку та ведення здорового способу життя.
	ПП 1. Здатність застосовувати законодавчу та нормативно-правову базу, а також державні та міжнародні вимоги, практики і стандарти з метою здійснення професійної діяльності в галузі інформаційної та кібербезпеки.
	ПП 6. Здатність відновлювати штатне функціонування інформаційних, інформаційно-телекомунікаційних (автоматизованих) систем після реалізації загроз , здійснення кібератак, збоїв та відмов різних класів та походження.
	ПП 8. Здатність здійснювати процедури управління інцидентами, проводити розслідування, надавати їм оцінку.
	ПП 11. Здатність виконувати моніторинг процесів функціонування інформаційних, інформаційно-телекомунікаційних (автоматизованих) систем згідно встановленої політики інформаційної та кібербезпеки.
	ПП 12. Здатність аналізувати, виявляти та оцінювати можливі загрози, уразливості та дестабілізуючі чинники інформаційному простору та інформаційним ресурсам згідно з встановленою політикою інформаційної та кібербезпеки.
Компетенції відповідно до вимог роботодавців	
1. Організація своєчасного виявлення, проведення оцінки і прогнозування джерел загроз інформаційній безпеці компанії; 2. Організація захисту від несанкціонованої модифікації і контролю цілісності використовуваних в корпоративній інформаційних системах компанії програмних засобів, а також захисту системи від впровадження несанкціонованих програм, включаючи шкідливе програмне забезпечення.	1. Здійснення моніторингу процесів і інструментів отримання, обробки і поширення інформації співробітниками компанії; 2. Здійснення моніторингу та контролю за дотриманням вимог до інформаційної безпеки співробітниками компанії на робочих місцях; 3. Проведення розслідувань за фактом інцидентів інформаційної безпеки.
6. Результати навчання відповідно до ОПП	
1. ПРН 15. Використовувати сучасне програмно-апаратне забезпечення інформаційно-комунікаційних технологій.	
2. ПРН 21. Вирішувати задачі забезпечення та супроводу (в.т. числі: огляд, тестування, підзвітність) системи управління доступом згідно встановленої політики безпеки в інформаційних та інформаційно-телекомунікаційних (автоматизованих) системах.	

3. ПРН 23. Реалізовувати заходи з протидії отриманню несанкціонованого доступу до інформаційних ресурсів і процесів в інформаційних та інформаційно-телекомунікаційних (автоматизованих) системах.
4. ПРН 24. Вирішувати задачі управління доступом до інформаційних ресурсів та процесів в інформаційних та інформаційно-телекомунікаційних (автоматизованих) системах на основі моделей управління доступом (мандатних, дискреційних, рольових).
5. ПРН 28. Аналізувати та проводити оцінку ефективності та рівня захищеності ресурсів різних класів в інформаційних та інформаційно-телекомунікаційних (автоматизованих) системах згідно встановленої політики інформаційної і кібербезпеки.
6. ПРН 34. Приймати участь у розробці та впровадженні стратегії інформаційної безпеки та кібербезпеки відповідно до цілей і завдань організації.
7. ПРН 41. Впроваджувати процеси виявлення, ідентифікації, аналізу та реагування на інциденти інформаційної і кібербезпеки.
8. ПРН 42. Застосовувати національні та міжнародні регулюючі акти в сфері інформаційної безпеки та кібербезпеки для розслідування інцидентів.
9. ПРН 45. Здійснювати аналіз та мінімізацію ризиків обробки інформації в інформаційно-телекомунікаційних системах.

7. План вивчення освітньої компоненти

Змістовний розділ	Вид заняття	Тема	Знати	Вміти	План заняття	Лекція, методична розробка
Розділ 1						
	Лекція 1	Тема: Предмет дисципліни “Цифрова криміналістика”. Моделі процесу розслідування кіберінцидентів.	1. Обґрунтування необхідності вивчення навчальної дисципліни “Цифрова криміналістика”. 2. Поняття “цифрова криміналістика”. Підходи науковців та практиків до визначення поняття “Цифрова криміналістика”. 3. Зміст процесу розслідування кіберінцидентів. Етапи процесу розслідування кіберінцидентів. 4. Цифрова криміналістична модель розслідування (Digital Forensic Investigation Model). 5. Інтегрована модель		http://dl.dut.edu.ua/course/view.php?id=614	http://dl.dut.edu.ua/course/view.php?id=614

			цифрового дослідження (The Integrated Digital Investigation Model (IDIP)).			
	Лекція 2	Тема: Поняття “реагування на кіберінциденти” (Incident Response). Поняття “цифрова криміналістика” (Digital Forensics).	1. Корпоративна інформаційна система як об’єкт захисту. 2. Превентивні, детективні та коректівні заходи забезпечення кібербезпеки сучасного підприємства. 3. Подія безпеки. Поняття уразливості. 4. Класифікація вразливостей. Джерела даних щодо вразливостей. Прийняті позначення вразливостей. 5. Поняття “реагування на кіберінциденти” (Incident Response). Основні етапи процесу реагування на інциденти та їх зміст. Основні рекомендації для організації правильного “реагування на кіберінциденти”. 6. Поняття “цифрова криміналістика”. Основні етапи розслідування кіберінцидентів та їх зміст.		http://dl.dut.edu.ua/course/view.php?id=614	http://dl.dut.edu.ua/course/view.php?id=614
	Лекція 3	Тема: Основи інформаційно-аналітичної діяльності фахівців з кібербезпеки. Місце інформаційно-аналітичної діяльності	1. Основи інформаційно-аналітичної діяльності фахівців з кібербезпеки. 2. Зміст інформаційно-аналітичної діяльності фахівців з кібербезпеки.		http://dl.dut.edu.ua/course/view.php?id=614	http://dl.dut.edu.ua/course/view.php?id=614

		фахівців з кібербезпеки в розслідуванні кіберінцидентів.				
	Лекція 4	Тема: Архітектура програмного комплексу IBM i2.	1. Логічна архітектура IBM i2 Analyze (дані, сервіси, клієнти). 2. Фізична архітектура IBM i2 Analyze. 3. Архітектура безпеки IBM i2 Analyze.		http://dl.dut.edu.ua/course/view.php?id=614	http://dl.dut.edu.ua/course/view.php?id=614
	Лекція 5	Тема: Основи застосування IBM i2 Analyst's Notebook. Дані в системі.	1. Дані в системі в IBM i2 Analyst's Notebook. 2. Об'єкти. 3. Зв'язки. 4. Властивості.		http://dl.dut.edu.ua/course/view.php?id=614	http://dl.dut.edu.ua/course/view.php?id=614
	Лекція 6	Тема: Основи застосування IBM i2 Analyst's Notebook. Схеми як основа візуального аналізу кіберінцидентів.	1. Схеми в IBM i2 Analyst's Notebook. 2. Створення схеми. 3. Відкриття схем. Копіювання схем. 4. Зміни властивостей схеми. 5. Аналітичні компонування схем. 6. Пошук інформації та мереж. 7. Статистичні представлення даних схеми.		http://dl.dut.edu.ua/course/view.php?id=614	http://dl.dut.edu.ua/course/view.php?id=614
	Лекція 7	Тема: Основи застосування IBM i2 Analyst's Notebook. Дослідження дій елемента.	1. Додавання елементів до Перегляду Активності (Activity View). 2. Інтерпретація даних дій. Зміна масштабу часу. 3. Пошук шаблонів дій. 4. Семантичний тип. Конфігурація індикаторів тривалості. Конфігурація		http://dl.dut.edu.ua/course/view.php?id=614	http://dl.dut.edu.ua/course/view.php?id=614

			форматування індикатора. 5. Обробка дій при неповних даних.			
	Лекція 8	Тема: Основи застосування IBM i2 Analyst's Notebook. Аналіз соціальної мережі.	1. Центральність і показники центральності (проміжність, проміжність зв’язків, близькість, ступінь, власний вектор, напрямок зв’язку, вага зв’язків, К-ядро). 2. Визначення показників кластеризації і центральності. Вибір показників центральності. 3. Додавання ваги зв'язків. 4. Робота зі сторінкою Результати.		http://dl.dut.edu.ua/course/view.php?id=614	http://dl.dut.edu.ua/course/view.php?id=614
	Лекція 9	Тема: Основи застосування IBM i2 Analyst's Notebook. Налаштування системи.	1. Основні можливості щодо налаштування системи Analyst's Notebook. 2. Інфотипи. 3. Користувальницькі семантичні типи. 4. Завдання загальних опцій програми. 5. Управління файлами і положеннями файлів. 6. Робота з модулями.		http://dl.dut.edu.ua/course/view.php?id=614	http://dl.dut.edu.ua/course/view.php?id=614
	Практичне заняття 1	Тема: Основні етапи процесу реагування на кіберінциденти та їх зміст.	1. Основні поняття в галузі кібербезпека. 2. Життєвий цикл атаки (kill chain). 3. Основні етапи процесу реагування на інциденти.		http://dl.dut.edu.ua/course/view.php?id=614	http://dl.dut.edu.ua/course/view.php?id=614
	Практичне заняття 2	Тема: Практичні дії фахівців за етапами процесу реагування на		1. Практичні дії фахівців на етапі підготовки до реагування на	http://dl.dut.edu.ua/course/view.php?id=614	http://dl.dut.edu.ua/course/view.php?id=614

		кіберінциденти.		кіберінциденти. 2. Практичні дії фахівців на етапі виявлення кіберінциденту. 2.1. Події кібербезпеки, які свідчать про можливі кіберінциденти. 2.2. Загальні вказівки щодо пріоритизації кіберінцидентів. 2.3. Інші фактори, на які слід звернути увагу при виявлення загрози. 2.4. Алгоритм аналізу подій в SIEM-системі. 3. Практичні дії фахівців на етапі стримування кіберінциденту. 3.1. Ізоляція інфікованих машин. 3.2. Зняття образів. 3.3. Переведення системи в режим роботи без ізольованих машин. 4. Практичні дії фахівців на етапі видалення та відновлення після кіберінциденту. 5. Практичні дії фахівців на етапі висновків після кіберінциденту.		
	Практичне заняття 3	Тема: Практичні дії фахівців за етапами APT-атаки.	1. Приклад змісту етапів APT-атаки. 2. Приклад (модель) мережевої інфраструктури банку.	Практичні дії фахівців за етапами APT-атаки.	http://dl.dut.edu.ua/course/view.php?id=614	http://dl.dut.edu.ua/course/view.php?id=614

			3. Процес виявлення APT-атаки. 4. Процес реагування на APT-атаку.			
	Практичне заняття 4	Тема: Дані в системі IBM i2 Analyst's Notebook. Робота зі схемами.		1. Дані в системі в IBM i2 Analyst's Notebook. Відображення даних. 2. Робота зі схемами в середовищі IBM i2 Analyst's Notebook.	http://dl.dut.edu.ua/course/view.php?id=614	http://dl.dut.edu.ua/course/view.php?id=614
	Практичне заняття 5	Тема: Імпорт даних у системі IBM i2 Analyst's Notebook.	1. Імпорт даних в форматі XML. 2. Імпорт даних в текстовому форматі або в форматі електронної таблиці.		http://dl.dut.edu.ua/course/view.php?id=614	http://dl.dut.edu.ua/course/view.php?id=614
	Практичне заняття 6	Тема: Робота IBM i2 Analyst's Notebook з IBM QRadar SIEM щодо розслідування порушень.	1. Спільна робота IBM QRadar SIEM з IBM i2 Analyst's Notebook. 2. Розширення даних про порушення, які додаються на схему із IBM QRadar SIEM. 3. Розширення IP-адрес, які додаються на схему із IBM QRadar SIEM.		http://dl.dut.edu.ua/course/view.php?id=614	http://dl.dut.edu.ua/course/view.php?id=614
	Практичне заняття 7	Тема: Дослідження активності елемента в середовищі IBM i2 Analyst's Notebook.		1 Додавання елементів до Перегляду Активності (Activity View). 2. Інтерпретація даних дій. Зміна масштабу часу. 3. Пошук шаблонів дій. 4. Семантичний тип. Конфігурація індикаторів тривалості. Конфігурація форматування індикатора. 5. Обробка дій при неповних даних.	http://dl.dut.edu.ua/course/view.php?id=614	http://dl.dut.edu.ua/course/view.php?id=614

	Практичне заняття 8	Тема: Аналіз соціальної мережі в середовищі IBM i2 Analyst's Notebook. Показники соціальної мережі.	1 Призначення методу аналізу соціальних мереж. 2. Показники, які застосовуються при аналізі соціальних мереж у Analyst's Notebook.		http://dl.dut.edu.ua/course/view.php?id=614	http://dl.dut.edu.ua/course/view.php?id=614
	Практичне заняття 9	Тема: Аналіз соціальної мережі в середовищі IBM i2 Analyst's Notebook. Робота з результатами аналізу соціальної мережі.	1 Робота з показниками кластеризації і центральності у Analyst's Notebook. 2. Робота з коефіцієнтами ваги зв'язків у Analyst's Notebook. 3. Робота з результатами аналізу у Analyst's Notebook.		http://dl.dut.edu.ua/course/view.php?id=614	http://dl.dut.edu.ua/course/view.php?id=614
	Лабораторне заняття 1	Тема: Основні етапи процесу реагування на кіберінциденти. Порядок реєстрації студентів у програмі IBM Academic Initiative. Система сертифікації фахівців з кібербезпеки компанією IBM.	1. Основні поняття в галузі кібербезпека. 2. Життєвий цикл атаки (kill chain). 3. Основні етапи процесу реагування на інциденти.	4. Порядок реєстрації студентів в програмі IBM Academic Initiative. Система сертифікації фахівців з кібербезпеки компанією IBM.	http://dl.dut.edu.ua/course/view.php?id=614	http://dl.dut.edu.ua/course/view.php?id=614
	Лабораторне заняття 2	Тема: Практичні дії фахівців за етапами процесу реагування на кіберінциденти.		1. Практичні дії фахівців на етапі підготовки до реагування на кіберінциденти. 2. Практичні дії фахівців на етапі виявлення кіберінциденту. 2.1. Події кібербезпеки, які свідчать про можливі кіберінциденти. 2.2. Загальні вказівки щодо пріоритизації кіберінцидентів.	http://dl.dut.edu.ua/course/view.php?id=614	http://dl.dut.edu.ua/course/view.php?id=614

				2.3. Інші фактори, на які слід звернути увагу при виявлення загрози. 2.4. Алгоритм аналізу подій в SIEM-системі. 3. Практичні дії фахівців на етапі стримування кіберінциденту. 3.1. Ізоляція інфікованих машин. 3.2. Зняття образів. 3.3. Переведення системи в режим роботи без ізольованих машин. 4. Практичні дії фахівців на етапі видалення та відновлення після кіберінциденту. 5. Практичні дії фахівців на етапі висновків після кіберінциденту.		
	Лабораторне заняття 3	Тема: Практичні дії фахівців за етапами APT-атаки.		1. Приклад змісту етапів APT-атаки. 2. Приклад (модель) мережевої інфраструктури банку. 3. Процес виявлення APT-атаки. 4. Процес реагування на APT-атаку.	http://dl.dut.edu.ua/course/view.php?id=614	http://dl.dut.edu.ua/course/view.php?id=614
	Лабораторне заняття 4	Тема: Інсталяція та розгортання системи IBM i2 Analyst's Notebook.		1. Інсталяція та розгортання системи IBM i2 Analyst's Notebook. 2. Ознайомлення з інтерфейсом програмного комплексу IBM i2 Analyst's	http://dl.dut.edu.ua/course/view.php?id=614	http://dl.dut.edu.ua/course/view.php?id=614

				Notebook.		
	Лабораторне заняття 5	Тема: Робота зі схемами в середовищі IBM i2 Analyst's Notebook.		1. Створення схеми. 2. Відкриття схем. Копіювання схем. 3. Аналітичні компонування схем. 4. Пошук інформації та мереж.	http://dl.dut.edu.ua/course/view.php?id=614	http://dl.dut.edu.ua/course/view.php?id=614
	Лабораторне заняття 6	Тема: Пошук даних та мереж в середовищі IBM i2 Analyst's Notebook.		1. Пошук даних. 2. Пошук мереж.	http://dl.dut.edu.ua/course/view.php?id=614	http://dl.dut.edu.ua/course/view.php?id=614
	Лабораторне заняття 7	Тема: Дослідження активності елемента в середовищі IBM i2 Analyst's Notebook.		1. Додавання елементів до Перегляду Активності (Activity View). 2. Інтерпретація даних дій. Зміна масштабу часу. 3. Пошук шаблонів дій.	http://dl.dut.edu.ua/course/view.php?id=614	http://dl.dut.edu.ua/course/view.php?id=614
	Лабораторне заняття 8	Тема: Дослідження активності елемента в середовищі IBM i2 Analyst's Notebook.		1. Семантичний тип. Конфігурація індикаторів тривалості. Конфігурація форматування індикатора. 2. Обробка дій при неповних даних.	http://dl.dut.edu.ua/course/view.php?id=614	http://dl.dut.edu.ua/course/view.php?id=614
	Лабораторне заняття 9	Тема: Аналіз соціальної мережі в середовищі IBM i2 Analyst's Notebook. Робота з результатами аналізу соціальної мережі.		1. Робота з показниками кластеризації і центральності у Analyst's Notebook. 2. Робота з коефіцієнтами ваги зв’язків у Analyst's Notebook. 3. Розрахунок значень показників соціальних мереж в середовищі Analyst's Notebook.	http://dl.dut.edu.ua/course/view.php?id=614	http://dl.dut.edu.ua/course/view.php?id=614
	Самостійна робота	Тема: Предмет дисципліни “Цифрова	1. Обґрунтування необхідності вивчення		http://dl.dut.edu.ua/course/view.php?id=614	http://dl.dut.edu.ua/course/view.php?id=614

		криміналістика”. Моделі процесу розслідування кіберінцидентів.	навчальної дисципліни “Цифрова криміналістика”. 2. Поняття “цифрова криміналістика”. Підходи науковців та практиків до визначення поняття “Цифрова криміналістика”. 3. Зміст процесу розслідування кіберінцидентів. Етапи процесу розслідування кіберінцидентів. 4. Цифрова криміналістична модель розслідування (Digital Forensic Investigation Model). 5. Інтегрована модель цифрового дослідження (The Integrated Digital Investigation Model (IDIP)).			
	Самостійна робота	Тема: Поняття “реагування на кіберінциденти” (Incident Response). Поняття “цифрова криміналістика” (Digital Forensics).	1. Корпоративна інформаційна система як об’єкт захисту. 2. Превентивні, детективні та коректівні заходи забезпечення кібербезпеки сучасного підприємства. 3. Подія безпеки. Поняття уразливості. 4. Класифікація вразливостей. Джерела даних щодо вразливостей. Прийняті позначення вразливостей. 5. Поняття “реагування на		http://dl.dut.edu.ua/course/view.php?id=614	http://dl.dut.edu.ua/course/view.php?id=614

			кіберінциденти” (Incident Response). Основні етапи процесу реагування на інциденти та їх зміст. Основні рекомендації для організації правильного “реагування на кіберінциденти”. 6. Поняття “цифрова криміналістика”. Основні етапи розслідування кіберінцидентів та їх зміст.			
	Самостійна робота	Тема: Основи інформаційно-аналітичної діяльності фахівців з кібербезпеки. Місце інформаційно-аналітичної діяльності фахівців з кібербезпеки в розслідуванні кіберінцидентів.	1. Основи інформаційно-аналітичної діяльності фахівців з кібербезпеки. 2. Зміст інформаційно-аналітичної діяльності фахівців з кібербезпеки.		http://dl.dut.edu.ua/course/view.php?id=614	http://dl.dut.edu.ua/course/view.php?id=614
	Самостійна робота	Тема: Архітектура програмного комплексу IBM i2.	1. Логічна архітектура IBM i2 Analyze (дані, сервіси, клієнти). 2. Фізична архітектура IBM i2 Analyze. 3. Архітектура безпеки IBM i2 Analyze.		http://dl.dut.edu.ua/course/view.php?id=614	http://dl.dut.edu.ua/course/view.php?id=614
	Самостійна робота	Тема: Основи застосування IBM i2 Analyst's Notebook. Дані в системі.	1. Дані в системі в IBM i2 Analyst's Notebook. 2. Об'єкти. 3. Зв'язки. 4. Властивості.	1. Дані в системі в IBM i2 Analyst's Notebook. Відображення даних. 2. Робота зі схемами в середовищі IBM i2 Analyst's Notebook.	http://dl.dut.edu.ua/course/view.php?id=614	http://dl.dut.edu.ua/course/view.php?id=614
	Самостійна робота	Тема: Основи застосування IBM i2	1. Схеми в IBM i2 Analyst's Notebook.	Робота зі схемами в середовищі IBM i2	http://dl.dut.edu.ua/course/view.php?id=614	http://dl.dut.edu.ua/course/view.php?id=614

		Analyst's Notebook. Схеми як основа візуального аналізу кіберінцидентів.	2. Створення схеми. 3. Відкриття схем. Копіювання схем. 4. Зміни властивостей схеми. 5. Аналітичні компонування схем. 6. Пошук інформації та мереж. 7. Статистичні представлення даних схеми.	Analyst's Notebook.		
	Самостійна робота	Тема: Основи застосування IBM i2 Analyst's Notebook. Дослідження дій елемента.	1. Додавання елементів до Перегляду Активності (Activity View). 2. Інтерпретація даних дій. Зміна масштабу часу. 3. Пошук шаблонів дій. 4. Семантичний тип. Конфігурація індикаторів тривалості. Конфігурація форматування індикатора. 5. Обробка дій при неповних даних.	Порядок дослідження дій елемента в середовищі IBM i2 Analyst's Notebook.	http://dl.dut.edu.ua/course/view.php?id=614	http://dl.dut.edu.ua/course/view.php?id=614
	Самостійна робота	Тема: Основи застосування IBM i2 Analyst's Notebook. Аналіз соціальної мережі.	1. Центральність і показники центральності (проміжність, проміжність зв'язків, близькість, ступінь, власний вектор, напрямок зв'язку, вага зв'язків, К-ядро). 2. Визначення показників кластеризації і центральності. Вибір показників центральності. 3. Додавання ваги зв'язків. 4. Робота зі сторінкою Результати.	1. Робота з показниками кластеризації і центральності у Analyst's Notebook. 2. Робота з коефіцієнтами ваги зв'язків у Analyst's Notebook. 3. Розрахунок значень показників соціальних мереж в середовищі Analyst's Notebook.	http://dl.dut.edu.ua/course/view.php?id=614	http://dl.dut.edu.ua/course/view.php?id=614
	Самостійна	Тема: Основи	1. Основні можливості щодо	Практичні дії з	http://dl.dut.edu	http://dl.dut.edu.ua/c

	робота	застосування IBM i2 Analyst's Notebook. Налаштування системи.	налаштування системи Analyst's Notebook. 2. Інфотипи. 3. Користувальницькі семантичні типи. 4. Завдання загальних опцій програми. 5. Управління файлами і положеннями файлів. 6. Робота з модулями.	налаштування системи IBM i2 Analyst's Notebook.	.ua/course/view .php?id=614	ourse/view.php?id=6 14
Розділ 2						
	…	…				
Розділ …						
	…	…				

8. Мова вивчення освітньої компоненти

(українська, англійська, розділи, що викладаються англійською мовою)

українська

9. Інформаційне забезпечення освітньої компоненти

Рекомендовані джерела та інші навчальні ресурси: вказати підручники, навчальні посібники не пізніше 2010 року видання, які є у нас у бібліотеці на державній мові; електронні ресурси, посилання, електронна бібліотека ДУТ, іншомовні джерела

1. Бурячок В.Л. Інформаційна та кібербезпека: соціотехнічний аспект: підручник / [В.Л. Бурячок, В.Б. Толубко, В.О. Хорошко, С.В. Толюпа]; за заг. ред. д-ра техн. наук, професора В.Б. Толубка. – К.: ДУТ, 2015.– 288 с.
2. Computer Security Incident Handling Guide. Recommendations of the National Institute of Standards and Technology. NIST Special Publication 800-61 Revision 2. Paul R. Cichonski, Thomas Millar, Timothy Grance, Karen Scarfone [Електронний ресурс]. Режим доступу: https://www.nist.gov/publications/computer-security-incident-handling-guide.
3. Smarter Cities Series: Understanding Fraud Investigation. Redguides for Business Leaders. James Luke. Tim Cooper. Rob Tucker [Електронний ресурс]. Режим доступу: http://www.redbooks.ibm.com/redpapers/pdfs/redp5037.pdf.
4. IBM i2 Integrated Law Enforcement:Technical Architecture and Deployment Guide. Wilfred (Wil) Jamison, John Dowlin. Redpaper [Електронний ресурс]. Режим доступу: http://www.redbooks.ibm.com/redpapers/pdfs/redp5130.pdf.
5. IBM i2 Enterprise Insight Analysis. Data Model. White Paper [Електронний ресурс]. Режим доступу: https://www.ibm.com/support/knowledgecenter/SSXVXZ_2.2.0/com.ibm.i2.understand.data.doc/platform_datamodel_whitepaper_pdf.pdf?origURL=SSXVXZ/com.ibm.i2.understand.data.doc/platform_datamodel_whitepaper_pdf.pdf.
6. IBM i2 Analyze. Architecture and Services. White Paper [Електронний ресурс]. Режим доступу: https://www.ibm.com/support/knowledgecenter/SS3J58_9.1.0/com.ibm.i2.admin.arch.doc/platform_architecture_whitepaper_external_pdf.pdf?origURL=SS3J58/com.ibm.i2.admin.arch.doc/platform_architecture_whitepaper_external_pdf.pdf.

7. IBM i2 Enterprise Insight Analysis. Security. White Paper [Електронний ресурс]. Режим доступу: https://www.ibm.com/support/knowledgecenter/SSXVXZ_2.1.8/com.ibm.i2.admin.security.doc/platform_security_whitepaper_pdf.pdf.
8. IBM i2 Intelligence Analysis Portfolio Product Access Management Guide. Version 9 Release 0. – 28 p.
9. IBM i2 Analyst's Notebook Social Network Analysis. Discover new insights and actionable intelligence from social network data. IBM Security. White Paper. March 2017 [Електронний ресурс]. Режим доступу: https://onaxion.nl/wp-content/uploads/2017/12/Social-Network-Analysis-IBM-Notebook.pdf#.
10. IBM i2 Enterprise Insight Analysis Understanding the Deployment Patterns [Електронний ресурс]. Режим доступу: https://www-01.ibm.com/support/docview.wss?uid=swg27049268&aid=1.

Інформаційний ресурс
IBM Knowledge Center. IBM i2 Analyst's Notebook 9.1. [Електронний ресурс]. Режим доступу: https://www.ibm.com/support/knowledgecenter/SSXVXZ_2.2.0/com.ibm.i2.anb.doc/analysts_notebook_welcome.html.

10. Методи оцінювання, підсумкові звітності за освітньою компонентою
(заліки, екзамени, курсові проекти, тестування)
іспит
11. Матеріально-технічне забезпечення освітньої компоненти
лабораторія «Кіберполігон» із програмним комплексом багатомірного візуального аналізу даних IBM i2 Analyst's Notebook