Інформаційний пакет освітніх компонент навчального плану
освітньо-професійної програми «ІНФОРМАЦІЙНА ТА КІБЕРНЕТИЧНА БЕЗПЕКА»
(назва)

Освітнього рівня перший (бакалавр)

Спеціальності 125 “Кібербезпека”

Галузь знань 12 Інформаційні технології

1. Назва освітньої компоненти “Основи захисту конфіденційних даних”
(назва дисципліни)

2. Тип основна

3. Обсяг:	Кредитів ECTS	Годин	За видами занять:				
			Лекцій	Семінар	Практичних занять	Лабораторних занять	Самостійна підготовка
	4	120	18	-	18	-	84
4. Взаємозв’язок у структурно-логічній схемі							
Освітні компоненти, які передують вивченню	1. Безпека безпроводових, мобільних та хмарних технологій 2. Аналіз та оцінка уразливостей інформаційних систем						
Освітні компоненти для яких є базовою	1. Комп'ютерні мережі 2. Теоретичні основи захищених інформаційно-комунікаційних технологій						
5. Компетенції відповідно до ОПП та вимог роботодавців:							
Компетенції відповідно до ООП							
Знати			**Вміти**				
1. законодавчу та нормативно-правову базу, а також державні та міжнародні вимоги, практики і стандарти з метою здійснення професійної діяльності в галузі інформаційної та кібербезпеки.			1. застосовувати знання у практичних ситуаціях				
2. як виявляти, ставити та вирішувати проблеми за професійним спрямуванням.			2. професійно спілкуватися державною та іноземною мовами як усно, так і письмово.				

3. як аналізувати, виявляти та оцінювати можливі загрози, уразливості та дестабілізуючі чинники інформаційному простору та інформаційним ресурсам згідно з встановленою політикою інформаційної та кібербезпеки.	3. здійснювати процедури управління інцидентами, проводити розслідування, надавати їм оцінку.
4. відновлювати штатне функціонування інформаційних, інформаційно-телекомунікаційних (автоматизованих) систем після реалізації загроз , здійснення кібератак, збоїв та відмов різних класів та походження.	4. здійснювати професійну діяльність на основі впровадженої системи управління інформаційною та кібербезпекою.
5. забезпечувати неперервність бізнесу згідно встановленої політики інформаційної та кібербезпеки.	5. виконувати моніторинг процесів функціонування інформаційних, інформаційно-телекомунікаційних (автоматизованих) систем згідно встановленої політики інформаційної та кібербезпеки.
Компетенції відповідно до вимог роботодавців	
1. Здатність застосовувати знання у практичних ситуаціях.	1. Вміння виявляти, ставити та вирішувати проблеми за професійним спрямуванням.
2. Здатність професійно спілкуватися державною та іноземною мовами як усно, так і письмово.	2. Здатність здійснювати процедури управління інцидентами, проводити розслідування, надавати їм оцінку.
3. 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.	3. Здатність відновлювати штатне функціонування інформаційних, інформаційно-телекомунікаційних (автоматизованих) систем після реалізації загроз , здійснення кібератак, збоїв та відмов різних класів та походження.
4. Здатність забезпечувати неперервність бізнесу згідно встановленої політики інформаційної та кібербезпеки.	4. Здатність здійснювати професійну діяльність на основі впровадженої системи управління інформаційною та кібербезпекою.
5. Здатність аналізувати, виявляти та оцінювати можливі загрози, уразливості та дестабілізуючі чинники інформаційному простору та інформаційним ресурсам згідно з встановленою політикою інформаційної та кібербезпеки.	5. Здатність виконувати моніторинг процесів функціонування інформаційних, інформаційно-телекомунікаційних (автоматизованих) систем згідно встановленої політики інформаційної та кібербезпеки.
6. Результати навчання відповідно до ОПП	
1. Адаптуватися в умовах частої зміни технологій професійної діяльності, прогнозувати кінцевий результат.	
2. Готувати пропозиції до нормативних актів щодо забезпечення інформаційної та кібербезпеки.	
3. Використовувати сучасне програмно-апаратне забезпечення інформаційно-комунікаційних технологій.	
4. Вирішувати задачі управління процедурами ідентифікації, автентифікації, авторизації процесів і користувачів в інформаційно-телекомунікаційних системах згідно встановленої політики інформаційної і кібербезпеки.	
5. Реалізовувати заходи з протидії отриманню несанкціонованого доступу до інформаційних ресурсів і процесів в інформаційних та інформаційно-телекомунікаційних (автоматизованих) системах.	
6. Вирішувати задачі управління доступом до інформаційних ресурсів та процесів в інформаційних та інформаційно-телекомунікаційних	

(автоматизованих) системах на основі моделей управління доступом (мандатних, дискреційних, рольових).						
7. Вирішувати задачі захисту потоків даних в інформаційних, інформаційно-телекомунікаційних (автоматизованих) системах.						
8. Здійснювати оцінювання можливості несанкціонованого доступу до елементів інформаційно-телекомунікаційних систем.						
7. План вивчення освітньої компоненти						
Змістовний розділ	Вид заняття	Тема	Знати	Вміти	План заняття	Лекція, методична розробка
	Лекція 1	Тема: Основи інформаційної безпеки. Загрози безпеки інформації	Різновиди мережевого обладнання та середовища передачі інформації	Готувати пропозиції до нормативних актів щодо забезпечення інформаційної та кібербезпеки.	http://moodle.duikt.edu.ua	http://moodle.duikt.edu.ua
	Лекція 2	Тема: Поняття конфіденційних даних	1. Закон України «про захист персональних даних» 2. Особливості даних, які відносяться до конфіденційної таємниці.	Нормативно забезпечити сертифікацію й атестацію технічних засобів захисту і контролювати їх ефективність	http://moodle.duikt.edu.ua	http://moodle.duikt.edu.ua
	Лекція 3	Тема: Особливості роботи з персоналом який володіє конфіденційною інформацією	1. Нормативні документи та розпізнавати присвоєні статуси доступу. 2. Різновид атак та вірусів, що здатні здійснювати негативні дії на конфіденційну інформацію	Організаційними методами забезпечити захист інформації з обмеженим доступом.	http://moodle.duikt.edu.ua	http://moodle.duikt.edu.ua
	Лекція 4	Тема: Організація робіт по проведенню контролю системи технічного захисту інформації	1. Системи захисту інформації. 2. Особливості використання алгоритмів цифрового підпису що здатні забезпечувати безпеку конфіденційних даних	1. Виконувати аналіз стану об’єкту захисту, виявляти ймовірні канали витоку інформації; 2. Працювати та налагоджувати різне мережеве обладнання	http://moodle.duikt.edu.ua	http://moodle.duikt.edu.ua
	Лекція 5	Тема: Криптографічні алгоритми цифрових підписів, стійкість яких засновується на використанні дискретних	1. Криптографічні алгоритми. 2. Ознайомитися із основними сферами використання	Здійснювати шифрування даних (повідомлень) з використанням класичних шифрів	http://moodle.duikt.edu.ua	http://moodle.duikt.edu.ua

		логарифмів				
	Лекція 6	Тема: Організація захисту інформації по матеріально-речовому каналу витоку за допомогою простих технічних засобів.	1. Канали витоку інформації 2. Особливості захисту інформації 3. Способи веб хакінгу	Виконувати передачу конфіденційних даних	http://moodle.duikt.edu.ua	http://moodle.duikt.edu.ua
	Лекція 7	Тема: Мережеві пристрої та протоколи, що забезпечують захист конфіденційних даних	1. Мультисервісні технології. 2. Активне та пасивне обладнання. 3. Особливості використання маршрутизаторів	Організувати прості топології з використанням брандмауерів	http://moodle.duikt.edu.ua	http://moodle.duikt.edu.ua
	Лекція 8	Тема: Вивчення особливостей побудови багаторівневої безпеки конфіденційних даних за допомогою обладнання Cisco	1. Особливості використання Cisco Umbrella. 2. Алгоритм дії	Оцінювати складність обчислень, визначати клас складності задачі	http://moodle.duikt.edu.ua	http://moodle.duikt.edu.ua
	Лекція 9	Тема: вивчення протоколів маршрутизації для безпечної передачі пакетів даних	1. Призначення та класифікація протоколів маршрутизації 2. Огляд протоколів маршрутизації	1. Здійснювати перевірку достовірності отриманої інформації; 2. Взаємодіяти із можливими алгоритмами кодування та декодування даних	http://moodle.duikt.edu.ua	http://moodle.duikt.edu.ua
	Практичне заняття 1	Тема: Налаштування паролів для доступу з програмою Cisco Packet Tracer	Призначення та можливості програми «Cisco Packet Tracer»	Побудувати, зконфігурувати та перевірити роботу найпростішої обчислювальної мережі, що складається з двох комп'ютерів.	http://moodle.duikt.edu.ua	http://moodle.duikt.edu.ua
	Практичне заняття 2	Тема: Налагодження базових	Проблеми безпеки інформаційних технології;	Дослідити організацію та особливості налагодження	http://moodle.duikt.e	http://moodle.duikt.edu.ua

		параметрів безпеки для комутаторів Cisco.	основні класичні шифри для шифрування даних (повідомлень).	базових засобів захисту комунікаційних пристроїв у мережі на базі обладнання фірми Cisco	du.ua	
	Практичне заняття 3	Тема: Організацію налагодження базових засобів захисту маршрутизаторів мережі на базі обладнання фірми Cisco	Принципи побудови дозвільної системи доступу до конфіденційної інформації	Виконувати аналіз стану об'єкту захисту.	http://moodle.duikt.edu.ua	http://moodle.duikt.edu.ua
	Практичне заняття 4	Тема: Захоплення пароля із застосуванням атаки ARP-spoofing	Дії системи захисту інформації в екстремальних умовах	Виявляти ймовірні канали витоку інформації.	http://moodle.duikt.edu.ua	http://moodle.duikt.edu.ua
	Практичне заняття 5	Тема: Фіксація хакерскої атаки на рівні мережевого обладнання за допомогою програмного забезпечення WINPCAP»	Основні міжнародні стандарти в сфері захисту інформації	Працювати та налагоджувати різне мережеве обладнання	http://moodle.duikt.edu.ua	http://moodle.duikt.edu.ua
	Практичне заняття 6	Тема: Злом хеш-функції пароля enable маршрутизатора Cisco	Існуючі способи забезпечення захисту конфіденційних даних в сучасних мультисервісних мережах.	Забезпечити сертифікацію й атестацію технічних засобів захисту.	http://moodle.duikt.edu.ua	http://moodle.duikt.edu.ua
	Практичне заняття 7	Тема: Підміна MAC-адрес. Вивчення особливостей фізичних та мережевих адрес	Основні різновиди атак, негативних впливів, чинників, що здатні нанести шкоди конфіденційним даним	Взаємодіяти із можливими алгоритмами кодування та декодування даних.	http://moodle.duikt.edu.ua	http://moodle.duikt.edu.ua
	Практичне заняття 8	Тема: Налаштування параметрів безпеки браузерів. Вивчення особливостей фізичних фаєрволів	Принципи побудови дозвільної системи доступу до конфіденційної інформації.	Здійснювати шифрування даних (повідомлень) з використанням класичних шифрів.	http://moodle.duikt.edu.ua	http://moodle.duikt.edu.ua
	Практичне заняття 9	Тема: Налаштування міжмережевого екрану	Дії системи захисту інформації в екстремальних	Організувати прості топології з використанням	http://moodle.duikt.e	http://moodle.duikt.edu.ua

		Cisco ASA	умовах.	брандмауерів.	du.ua	
	Самостійна робота	Тема 1. Модель OSI. Тема 2. Середовища передачі інформації Тема 3. MAC-адресація Тема 4. Призначення VPN. Тема 5. Протокол DHCP Тема 6. Мережева функція NAT Тема 7. Організація СУБД Тема 8. Особливості блокування запитів Тема 9. Різновиди антивірусного програмного забезпечення Тема 10. Взаємодія із брандмауерами Cisco Тема 11.Протокол RIP, BGP Тема 12. Алгоритми криптографічного захисту	1. Проблеми безпеки інформаційних технології; основні класичні шифри для шифрування даних (повідомлень); 2. Принципи поточної роботи з персоналом який володіє конфіденційною інформацією; 3. Принципи побудови дозвільної системи доступу до конфіденційної інформації; 4. Дії системи захисту інформації в екстремальних умовах, 5. Основні міжнародні стандарти в сфері захисту інформації; 6. Основні різновиди атак, негативних впливів, чинників, що здатні нанести шкоди конфіденційним даним; 7. Принципи формування систем захисту інформації; 8. Існуючі способи забезпечення захисту конфіденційних даних в сучасних мультисервісних мережах.	1. Виконувати аналіз стану об’єкту захисту; 2. Виявляти ймовірні канали витоку інформації; 3. Забезпечити захист інформації з обмеженим доступом. 4. Забезпечити сертифікацію й атестацію технічних засобів захисту. 5. Контролювати їх ефективність; 6. Здійснювати шифрування даних (повідомлень) з використанням класичних шифрів; 7. Організувати прості топології з використанням брандмауерів; 8. Виконувати передачу конфіденційних даних; 9. Працювати та налагоджувати різне мережеве обладнання; 10. Здійснювати перевірку достовірності отриманої інформації; 11. Взаємодіяти із можливими алгоритмами кодування та декодування даних.	http://moodle.duikt.edu.ua	http://moodle.duikt.edu.ua
8. Мова вивчення освітньої компоненти						
Українська						

9. Інформаційне забезпечення освітньої компоненти
1. Навчальний сайт університету - http://moodle.duikt.edu.ua
2. Бем М. В., Городиський І. М., Саттон Г., Родіоненко О. М. Захист персональних даних: Правове регулювання та практичні аспекти: науково-практичний посібник. – К.: К.І.С., 2015. – 220 с.
3. Hoffstein J., Pipher J., Silverman J. Fn introduction to mathematical cryptography.Springer, 2014.
4. Сучасні методи та моделі обробки даних в інформаційних системах : монографія / О. М. Беседовський, І. О. Золотарьова, С. П. Євсеєв та ін.; за заг. ред. докт. екон. наук, професора Пономаренка В. С. – Х. : Вид. ХНЕУ ім. С. Кузнеця, 2013. – 540 с. (Укр. мов.)
5. ДСТУ 4145-2002 "Інформаційні технології. Криптографічний захист інформації. Цифровий підпис, що ґрунтується на еліптичних кривих. Формування та перевіряння".
6. ДСТУ 7624:2014 "Інформаційні технології. Криптографічний захист інформації. Алгоритм симетричного блокового перетворення".
7. ДСТУ 7564:2014 "Інформаційні технології. Криптографічний захист інформації. Функція гешування".
10. Методи оцінювання, підсумкові звітності за освітньою компонентою
екзамен
11. Матеріально-технічне забезпечення освітньої компоненти

Інформаційний пакет освітньої компоненти, яка викладається англійською мовою, додатково розміщується на сторінці кафедри на англійській мові