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

Освітнього рівня **бакалавр**

Спеціальності **125 «Кібербезпека»**

Галузь знань **12 «Інформаційні технології»**

1. Назва освітньої компоненти Стандарти криптографічного захисту
(назва дисципліни)

2. Тип основна

3. Обсяг:	Кредитів ECTS	Годин	За видами занять:				
			Лекцій	Семінар	Практичних занять	Лабораторних занять	Самостійна підготовка
	4	120	36		36		48
4. Взаємозв'язок у структурно-логічній схемі							
Освітні компоненти, які передують вивченню	1. Теоретичні основи захищених інформаційно-комунікаційних технологій 2. Прикладна криптологія						
Освітні компоненти для яких є базовою	1. Комплексні системи захисту інформації 2. Кібербезпека банківських та комерційних структур						
5. Компетенції відповідно до ОПП та вимог роботодавців:							
Компетенції відповідно до ООП							
Знати			**Вміти**				
1. Здатність застосовувати знання у практичних ситуаціях.			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.				
2. Здатність до пошуку, оброблення та аналізу інформації.			2. Здатність застосовувати методи та засоби криптографічного та технічного захисту інформації на об'єктах інформаційної діяльності.				

Компетенції відповідно до вимог роботодавців	
1. Знання законодавчої та нормативно-правової бази, а також державних та міжнародних вимог, практик і стандартів з метою здійснення професійної діяльності в галузі інформаційної та/або кібербезпеки.	1. Здатність застосовувати законодавчу та нормативно-правову базу, а також державні та міжнародні вимоги, практики і стандарти з метою здійснення криптографічного захисту інформації; застосовувати методи та засоби криптографічного захисту інформації на об'єктах інформаційної діяльності
	2. Здатність діяти на основі законодавчої та нормативно-правової бази України та вимог відповідних стандартів, у тому числі міжнародних в галузі криптографічного захисту
	3. Здатність готувати пропозиції до нормативних актів щодо забезпечення криптографічного захисту інформації.

6. Результати навчання відповідно до ОПП

1. Застосовувати знання державної та іноземних мов з метою забезпечення ефективності професійної комунікації.
2. Діяти на основі законодавчої та нормативно-правової бази України та вимог відповідних стандартів, тому числі міжнародних в галузі інформаційної та кібербезпеки.
3. Вирішувати задачі захисту інформації, що обробляється в інформаційно-телекомунікаційних системах з використанням сучасних методів та засобів криптографічного захисту інформації.
4. Виконувати впровадження та підтримку систем виявлення вторгнень та використовувати компоненти криптографічного захисту для забезпечення необхідного рівня захищеності інформації в інформаційно-телекомунікаційних системах.

7. План вивчення освітньої компоненти

Змістовний розділ	Вид заняття	Тема	Знати	Вміти	План заняття	Лекція, методична розробка
	Лекція 1	Тема: Введення в дисципліну.	1. Роль і місце курсу в загальній системі підготовки бакалавра. 2. Об'єкти і предмети вивчення дисципліни. 3. Загальну структуру курсу			http://dl.dut.edu.ua/course/view.php?id=1598
	Лекція 2	Тема: Основні поняття та терміни криптології. Основи стандартизації України.	1. Основні поняття та терміни криптології. 2. Основи стандартизації України			
	Практичне заняття 1	Тема: Основні поняття та терміни криптології.		Застосовувати основні поняття та терміни		

		Основи стандартизації України.		криптології; основи стандартизації України.		
	Лекція 3	Тема: Стандарт шифрування даних DES (3DES).	1. Сутність стандарту шифрування даних DES (3DES). 2. Зміст стандарту шифрування даних DES (3DES). 3. Галузь використання стандарту шифрування даних DES (3DES).			http://dl.dut.edu.ua/course/view.php?id=1598
	Практичне заняття 2	Тема: Стандарт шифрування даних DES (3DES).		Застосовувати стандарт шифрування даних DES (3DES) на об’єктах інформаційної діяльності.		http://dl.dut.edu.ua/course/view.php?id=1598
	Лекція 4	Тема: Стандарт шифрування даних AES.	1. Сутність стандарту шифрування даних AES 2. Зміст стандарту шифрування даних AES 3. Галузь використання стандарту шифрування даних AES			http://dl.dut.edu.ua/course/view.php?id=1598
	Практичне заняття 3	Тема: Стандарт шифрування даних AES..		Застосовувати стандарт шифрування даних AES на об’єктах інформаційної діяльності.		http://dl.dut.edu.ua/course/view.php?id=1598
	Лекція 5	Тема: ДСТУ 4145-2002 Інформаційні технології. Криптографічний захист інформації. Цифровий підпис, що ґрунтується на еліптичних кривих. Формування та перевірка.	1. Сутність стандарту шифрування даних ДСТУ 4145-2002. 2. Зміст стандарту шифрування даних ДСТУ 4145-2002. 3. Галузь використання стандарту шифрування даних ДСТУ 4145-2002.			http://dl.dut.edu.ua/course/view.php?id=1598
	Практичне	Тема: ДСТУ 4145-2002		Застосовувати стандарт		http://dl.dut.e

	заняття 4	Інформаційні технології. Криптографічний захист інформації. Цифровий підпис, що ґрунтується на еліптичних кривих. Формування та перевірка.		ДСТУ 4145-2002		du.ua/course/view.php?id=1598
	Лекція 6	Тема: ДСТУ 28147-2009 Система обробки інформації. Захист криптографічний. Алгоритм криптографічного перетворення (ГОСТ 28147-89).	1. Сутність стандарту шифрування даних ДСТУ 28147-2009. 2. Зміст стандарту шифрування даних ДСТУ 28147-2009. 3. Галузь використання стандарту шифрування даних ДСТУ 28147-2009.			http://dl.dut.edu.ua/course/view.php?id=1598
	Практичне заняття 5	Тема: ДСТУ 28147-2009 Система обробки інформації. Захист криптографічний. Алгоритм криптографічного перетворення (ГОСТ 28147-89).		Застосовувати стандарт ДСТУ 28147-2009		http://dl.dut.edu.ua/course/view.php?id=1598
	Лекція 7	Тема: ДСТУ 7624:2014 "Інформаційні технології. Криптографічний захист інформації. Алгоритм симетричного блокового перетворення".	1. Сутність стандарту шифрування даних ДСТУ 7624:2014 . 2. Зміст стандарту шифрування даних ДСТУ 7624:2014. 3. Галузь використання стандарту шифрування даних ДСТУ 7624:2014			http://dl.dut.edu.ua/course/view.php?id=1598
	Практичне заняття 6	Тема: ДСТУ 7624:2014 "Інформаційні технології.		Застосовувати стандарт ДСТУ 7624:2014		http://dl.dut.edu.ua/course/

		Криптографічний захист інформації. Алгоритм симетричного блокового перетворення".				view.php?id=1598
	Лекція 8	Тема: ДСТУ 7564:2014 "Інформаційні технології. Криптографічний захист інформації. Функція гешування".	1. Сутність стандарту шифрування даних ДСТУ 7564:2014. 2. Зміст стандарту шифрування даних ДСТУ 7564:2014. 3. Галузь використання стандарту шифрування даних ДСТУ 7564:2014.			http://dl.dut.edu.ua/course/view.php?id=1598
	Практичне заняття 7	Тема: ДСТУ 7564:2014 "Інформаційні технології. Криптографічний захист інформації. Функція гешування".		Застосовувати стандарт ДСТУ 7564:2014		http://dl.dut.edu.ua/course/view.php?id=1598
	Лекція 9	Тема: ГОСТ Р 34.12-2015. “Інформаційна технологія. Криптографічний захист інформації. Блокові шифри”.	1. Сутність стандарту шифрування даних ГОСТ Р 34.12-2015. 2. Зміст стандарту шифрування даних ГОСТ Р 34.12-2015. 3. Галузь використання стандарту шифрування даних ГОСТ Р 34.12-2015.			http://dl.dut.edu.ua/course/view.php?id=1598
	Практичне заняття 8	Тема: ГОСТ Р 34.12-2015. “Інформаційна технологія. Криптографічний захист інформації. Блокові шифри”.		Застосовувати стандарт ГОСТ Р 34.12-2015		http://dl.dut.edu.ua/course/view.php?id=1598
	Лекція 10	Тема: Міжнародні стандарти криптографічного	1. Перелік міжнародних стандартів криптографічного захисту інформації.			http://dl.dut.edu.ua/course/view.php?id=

		захисту інформації.	2. Зміст міжнародних стандартів криптографічного захисту інформації. 3. Галузь використання міжнародних стандартів криптографічного захисту інформації.			1598
	Практичне заняття 9	Тема: Міжнародні стандарти криптографічного захисту інформації.		Застосовувати міжнародні стандарти криптографічного захисту інформації		http://dl.dut.edu.ua/course/view.php?id=1598

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. Технології захисту інформації [Електронний ресурс] : підручник / Ю. А. Тарнавський; КПІ ім. Ігоря Сікорського. – Електронні текстові дані (1 файл: 2,04 Мбайт). – Київ : КПІ ім. Ігоря Сікорського, 2018. – 162 с.

2. Національний стандарт України ДСТУ 4145-2002 "Інформаційні технології. Криптографічний захист інформації. Цифровий підпис, що ґрунтується на еліптичних кривих. Формування та перевірка".

3. Національний стандарт України ДСТУ 7624:2014 "Інформаційні технології. Криптографічний захист інформації. Алгоритм симетричного блокового перетворення".

4. Національний стандарт України ДСТУ 7564:2014 "Інформаційні технології. Криптографічний захист інформації. Функція гешування".

5. Національний стандарт України ДСТУ ГОСТ 28147:2009 "Системы обработки информации. Защита криптографическая. Алгоритмы криптографического преобразования".

6. ДСТУ ISO/IEC 9796-2:2015 Інформаційні технології. Методи захисту. Схеми цифрового підпису, які забезпечують відновлення повідомлення. Частина 2. Механізми, що ґрунтуються на факторизації цілих чисел (ISO/IEC 9796-2:2010, IDT)

7. ДСТУ ISO/IEC 9796-3:2015 Інформаційні технології. Методи захисту. Схеми цифрового підпису, які забезпечують відновлення повідомлення. Частина 3. Механізми, що ґрунтуються на дискретному логарифмі (ISO/IEC 9796-3:2006, IDT)

8. ДСТУ ISO/IEC 10118-2:2015 Інформаційні технології. Методи захисту. Геш-функції. Частина 2. Геш-функції, що використовують n-бітний блоковий шифр (ISO/IEC 10118-2:2010; Cor 1:2011, IDT)

9. ДСТУ ISO/IEC 10118-4:2015 Інформаційні технології. Методи захисту. Геш-функції. Частина 4. Геш-функції, що використовують модульну арифметику (ISO/IEC 10118-4:1998; Cor 1:2014; Amd 1:2014, IDT)

10. ДСТУ ISO/IEC 11770-1:2015 Інформаційні технології. Методи захисту. Керування ключами. Частина 1. Основні положення (ISO/IEC 11770-1:2010, IDT)

11. ДСТУ ISO/IEC 11770-2:2015 Інформаційні технології. Методи захисту. Керування ключами. Частина 2. Механізми з використанням симетричних методів (ISO/IEC 11770-2:2008; Cor 1:2009, IDT)

12. ДСТУ ISO/IEC 11770-3:2015 Інформаційні технології. Методи захисту. Керування ключами. Частина 3. Механізми з використанням асиметричних методів (ISO/IEC 11770-3:2008; Cor 1:2009, IDT)

13. ДСТУ ISO/IEC 11770-4:2015 Інформаційні технології. Методи захисту. Керування ключами. Частина 4. Механізми, засновані на нестійких секретах (ISO/IEC 11770-4:2008; Cor 1:2009, IDT)

14. ДСТУ ISO/IEC 11770-5:2015 Інформаційні технології. Методи захисту. Керування ключами. Частина 5. Керування груповими ключами (ISO/IEC 11770-5:2008, IDT)

15. ДСТУ ISO/IEC 13888-1:2015 Інформаційні технології. Методи захисту. Неспростовність. Частина 1. Загальні положення (ISO/IEC 13888-1:2009, IDT)

16. ДСТУ ISO/IEC 13888-2:2015 Інформаційні технології. Методи захисту. Неспростовність. Частина 2. Механізми з використанням симетричних методів (ISO/IEC 13888-2:2010; Cor 1:2012, IDT)

17. ДСТУ ISO/IEC 13888-3:2015 Інформаційні технології. Методи захисту. Неспростовність. Частина 3. Механізми з використанням асиметричних методівb(ISO/IEC 13888-3:2009, IDT)

18. ДСТУ ISO/IEC 14888-1:2015 Інформаційні технології. Методи захисту. Цифрові підписи з доповненням. Частина 1. Загальні положення (ISO/IEC 14888-1:2008, IDT)

19. ДСТУ ISO/IEC 14888-2:2015 Інформаційні технології. Методи захисту. Цифрові підписи з доповненням. Частина 2. Механізми, що ґрунтуються на факторизації цілих чисел (ISO/IEC 14888-2:2008, IDT)

20. ДСТУ ISO/IEC 14888-3:2015 Інформаційні технології. Методи захисту. Цифрові підписи з доповненням. Частина 3. Механізми, що ґрунтуються на дискретному логарифмуванні (ISO/IEC 14888-3:2006; Cor 1:2007; Cor 2:2009; Amd 1:2010; Amd 1:2012, IDT)

21. ДСТУ ISO/IEC 15946-1:2015 Інформаційні технології. Методи захисту. Криптографічні методи на основі еліптичних кривих. Частина 1. Загальні положення (ISO/IEC 15946-1:2008; Cor 1:2009; Cor 2:2014, IDT)

22. ДСТУ ISO/IEC 15946-5:2015 Інформаційні технології. Методи захисту. Криптографічні методи на основі еліптичних кривих. Частина 5. Генерація еліптичних кривих (ISO/IEC 15946-5:2009; Cor 1:2012, IDT)

23. ДСТУ ISO/IEC 18031:2015 Інформаційні технології. Методи захисту. Випадкова генерація біт (ISO/IEC 18031:2011; Cor 1:2014, IDT)

24. ДСТУ ISO/IEC 18032:2015 Інформаційні технології. Методи захисту. Покоління простих чисел (ISO/IEC 18032:2005, IDT)

25. ДСТУ ISO/IEC 18033-2:2015 Інформаційні технології. Методи захисту. Алгоритми шифрування. Частина 2. Асиметричні шифри (ISO/IEC 18033-2:2006, IDT)

26. ДСТУ ISO/IEC 18033-3:2015 Інформаційні технології. Методи захисту. Алгоритми шифрування. Частина 3. Блокові шифри (ISO/IEC 18033-3:2010, IDT)

27. ДСТУ ISO/IEC 18033-4:2015 Інформаційні технології. Методи захисту. Алгоритми шифрування. Частина 4. Потокові шифри (ISO/IEC 18033-4:2011, IDT)

28. ДСТУ ISO/IEC 19790:2015 Інформаційні технології. Методи захисту. Вимоги безпеки до криптографічних модулів (ISO/IEC 19790:2012, IDT)

29. ДСТУ ISO/IEC 24759:2015 Інформаційні технології. Методи захисту. Вимоги до випробувань криптографічних модулів (ISO/IEC 24759:2014, IDT)

30. ДСТУ ГОСТ 28147-2009 Система обробки інформації. Захист криптографічний. Алгоритм криптографічного перетворення (ГОСТ 28147-89) 31. ДСТУ ISO/IEC 29192-1:2015 Інформаційні технології. Методи захисту. Легка криптографія. Частина 1. Загальні положення (ISO/IEC 29192-1:2012, IDT) 32. ДСТУ ISO/IEC 29192-2:2015 Інформаційні технології. Методи захисту. Легка криптографія. Частина 2. Блокові шифри (ISO/IEC 29192-2:2012, IDT) 33. ДСТУ ISO/IEC 29192-3:2015 Інформаційні технології. Методи захисту. Легка криптографія. Частина 3. Потокові шифри (ISO/IEC 29192-3:2012, IDT) 34. ДСТУ ISO/IEC 29192-4:2015 Інформаційні технології. Методи захисту. Легка криптографія. Частина 4. Механізми щодо використання асиметричних методів (ISO/IEC 29192-4:2013, IDT) 35. ISO/IEC 10116: 2017 Информационные технологии. Методы безопасности. Режимы работы для n-разрядного блочного шифрования
10. Методи оцінювання, підсумкові звітності за освітньою компонентою
(заліки, екзамени, курсові проекти, тестування)
екзамен
11. Матеріально-технічне забезпечення освітньої компоненти
Макет ПК. Принтер HP. Жорсткий диск SATA, PATA.

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