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 Захист від шкідливого програмного засобу
(назва дисципліни)

2. Тип **основна**

3. Обсяг:	Кредитів ECTS	Годин	За видами занять:				
			Лекцій	Семінар	Практичних занять	Лабораторних занять	Самостійна підготовка
	5	90	18		18	18	36

4. Взаємозв'язок у структурно-логічній схемі	
Освітні компоненти, які передують вивченню	1. Стандарти інформаційної та кібербезпеки 2. Операційні системи 3. Комп'ютерні мережі 4. Прикладне програмування 5. Застосування інформаційно-телекомунікаційних засобів
Освітні компоненти для яких є базовою	1. Аналіз та оцінка уразливостей інформаційних систем 2. Безпека безпроводових, мобільних та хмарних технологій 3. Безпека Web-ресурсів 4. Інформаційна та кібербезпека сучасного підприємства 5. Кібербезпека банківських та комерційних структур 6. Комплексні системи захисту інформації 7. Методи та засоби протидії кіберзлочинності 8. Основи безпеки комп'ютерних мереж 9. Програмні комплекси захисту автоматизованих систем від несанкціонованого доступу

5. Компетенції відповідно до ОПП та вимог роботодавців:	
Компетенції відповідно до ООП	
Знати	**Вміти**
1. Здатність застосовувати знання у практичних ситуаціях.	1. Здатність забезпечувати захист інформації, що обробляється в інформаційно-телекомунікаційних (автоматизованих) системах з метою реалізації встановленої політики інформаційної та кібербезпеки.

2. Вміння виявляти, ставити та вирішувати проблеми за професійним спрямуванням.	2. Здатність відновлювати штатне функціонування інформаційних, інформаційно-телекомунікаційних (автоматизованих) систем після реалізації загроз, здійснення кібератак, збоїв та відмов різних класів та походження.
	3. Здатність здійснювати професійну діяльність на основі впровадженої системи управління інформаційною та кібербезпекою.
Компетенції відповідно до вимог роботодавців	
1. Знання сучасних загроз та ризиків інформаційної безпеки.	1. Мінімізація ризиків інформаційної безпеки при веденні операційної діяльності організації.
2. Знання з організації та забезпечення процесів управління інформаційною безпекою щодо сучасних загроз.	2. Проведення детального аналізу методів проникнення та видалення програм зі шкідливим та потенційно небезпечним діянням.
3. Сучасні загрози та ризики щодо інформаційної безпеки інформаційно-телекомунікаційних систем.	3. Застосування AVP і програмних, клієнт-серверних технологій щодо ЗІ від шкідливих програмних засобів та Spam
4. Знання основних загроз, навички виявлення, аналізу та основних способів поширення шкідливих програм.	4. Використання систем моніторингу програмних засобів, клієнт-серверних технологій захисту інформації.
5. Знання базових можливостей сучасних антивірусних програм (AVP).	
6. Розуміння особливостей роботи сучасного шкідливого програмного забезпечення.	

6. Результати навчання відповідно до ОПП

1. Адаптуватися в умовах частої зміни технологій професійної діяльності, прогнозувати кінцевий результат.
2. Вирішувати завдання захисту програм та інформації, що обробляється в інформаційно-телекомунікаційних системах програмно-апаратними засобами та давати оцінку якості прийнятих рішень.
3. Використовувати програмні та програмно-апаратні комплекси захисту інформаційних ресурсів.
4. Забезпечувати функціонування спеціального програмного забезпечення, щодо захисту інформації від руйнуючих програмних впливів, руйнуючих кодів в інформаційно-телекомунікаційних системах.
5. Забезпечувати функціонування програмних та програмно-апаратних комплексів виявлення вторгнень різних рівнів та класів (статистичних, сигнатурних, статистично-сигнатурних).
6. Використовувати інструментарій для моніторингу процесів в інформаційно-телекомунікаційних системах.
7. Вирішувати задачі аналізу програмного коду на наявність можливих уразливостей.

7. План вивчення освітньої компоненти

Змістовний розділ	Вид заняття	Тема	Знати	Вміти	План заняття	Лекція, методична розробка
Розділ 1. Сучасні аспекти захисту інформації в інформаційно-телекомунікаційних системах від руйнуючих програмних впливів.						
	Лекція 1	Тема: Сучасні напрями розвитку інформаційної та кібербезпеки щодо захисту від шкідливого програмного забезпечення.	1. Основи побудови комплексу засобів захисту від шкідливого програмного забезпечення (ШПЗ). 2. Сучасне небезпечне ШПЗ.		http://dl.dut.edu.ua/course/view.php?id=1595	http://dl.dut.edu.ua/course/view.php?id=1595

			3. Основи нормативно-правової бази щодо ІБ та кібербезпеки від загроз.			
	Лекція 2	Тема: Загальні поняття про шкідливі і потенційно небезпечні програмні засоби.	1. Існуючі види сучасного ШПЗ. 2. The emergence of epidemic of computer viruses (Brain, Lehigh, Jerusalem, Worm Morris, Datacrime). 3. Джерела загроз інформації, класифікації загроз.		http://dl.dut.edu.ua/course/view.php?id=1595	http://dl.dut.edu.ua/course/view.php?id=1595
	Лекція 3	Тема: Визначення та класифікація шкідливих програмних засобів та malicious software.	1. Визначення, класифікація ШПЗ. 2. Executable Files, Scripts, Configuration Files to mask event control objects data collection. 3. Найбільш небезпечні malicious software. 4. Model Computer Virus, Trojan-horse.		http://dl.dut.edu.ua/course/view.php?id=1595	http://dl.dut.edu.ua/course/view.php?id=1595
	Лекція 4	Тема: Негативний вплив Computer virus та Trojan-horse на програмно-апаратні засоби ІТС.	1. Прояв дій, засоби розповсюдження malicious software. 2. Характерні моделі поведінки. 3. Відмінні риси Computer Virus, Trojan-horse та malicious software.		http://dl.dut.edu.ua/course/view.php?id=1595	http://dl.dut.edu.ua/course/view.php?id=1595
	Практичне заняття 1	Тема: Оцінка нормативно-правової бази в області ЗІ від НСД та сучасних кіберзагроз.		Застосовувати знання і вміння для попередження небезпечних ризиків та сучасних кіберзагроз ІБ ІТС.	http://dl.dut.edu.ua/course/view.php?id=1595	http://dl.dut.edu.ua/course/view.php?id=1595
	Практичне заняття 2	Тема: Дослідження шкідливих та потенційно небезпечних засобів і їх властивостей.		Проводити аналіз технології впровадження і поширення malicious software та їх властивостей.	http://dl.dut.edu.ua/course/view.php?id=1595	http://dl.dut.edu.ua/course/view.php?id=1595
	Практичне заняття 3	Тема: Основи побудови комплексу засобів захисту (КЗЗ) від malicious software.		Володіти типовими підходами з комплексного забезпечення ІБ та засобами захисту від malicious software.	http://dl.dut.edu.ua/course/view.php?id=1595	http://dl.dut.edu.ua/course/view.php?id=1595
	Практичне заняття 4	Тема: Дослідження технологій сигнатурного,		1. Проводити оцінку ефективності сучасних AVP, їх	http://dl.dut.edu.ua/course/	http://dl.dut.edu.ua/course/

		імовірнісного аналізу та оцінка ефективності сучасних AVP.		можливостей. 2. Володіти основами проведення аналізу загроз технологіями сигнатурного, імовірнісного аналізу AVP.	view.php?id=1595	view.php?id=1595
	Лабораторне заняття 1	Тема: Дослідження методів та способів поширення malicious software.		1. Аналізувати існуючі технології, методи і засоби поширення malicious software. 2. Схеми дій.	http://dl.dut.edu.ua/course/view.php?id=1595	http://dl.dut.edu.ua/course/view.php?id=1595
	Лабораторне заняття 2	Тема: Дослідження засобів порушення інформаційної безпеки ІТС від malicious software та методи протидії.		Прогнозувати та вирішувати завдання ЗІ від malicious software відповідно до сучасних підходів.	http://dl.dut.edu.ua/course/view.php?id=1595	http://dl.dut.edu.ua/course/view.php?id=1595
	Лабораторне заняття 3	Тема: Основні ознаки присутності malicious software та методи запобігання типовим зараженням ІТС.		Вміння виявляти особливості ознак зараження ІТС шкідливим програмним забезпеченням.	http://dl.dut.edu.ua/course/view.php?id=1595	http://dl.dut.edu.ua/course/view.php?id=1595
Розділ 2. Технології та методи забезпечення безпеки інформації в ІТС від кібератак та руйнуючих програмних впливів.						
	Лекція 5	Тема: Механізми та засоби захисту від ШПЗ.	1. Класифікація AVP. 2. Переваги та недоліки AVP. 3. Особливості використання сучасних AVP. 4. Сучасні комплексні антивірусні системи в організаціях та підприємствах.		http://dl.dut.edu.ua/course/view.php?id=1595	http://dl.dut.edu.ua/course/view.php?id=1595
	Лекція 6	Тема: Механізми та засоби захисту операційних систем Windows/UNIX від ШПЗ.	1. Загрози від Exploits, rootkit, Worms для ОС Windows. 2. Структура, функції та реалізація засобів забезпечення захисту ОС від ШПЗ. 3. Адміністрування та механізми захисту ОС.		http://dl.dut.edu.ua/course/view.php?id=1595	http://dl.dut.edu.ua/course/view.php?id=1595

Виконано ст. викладачем Хмелевським Р.М.

	Лекція 7	Тема: Сучасні рішення щодо обміну та зберігання даних в ІТС сполученою з мережею Internet.	1. Технології TCP/IP, DNS, DHCP, SSL/TLS. 2. Типи та класифікації загроз в мережі. 3. Загрози типу DoS/DDoS. 4. Spam bot. Методи протидії. 5. Структура, функції та методи реалізації ЗЗІ від Spam attacks.		http://dl.dut.edu.ua/course/view.php?id=1595	http://dl.dut.edu.ua/course/view.php?id=1595
	Лекція 8	Тема: Перспективні напрями розвитку СЗІ в розподілених середовищах. Системи IDS/IPS світових виробників.	1. Основні характеристики, преваги та недоліки IDS/IPS. 2. Сучасні систем IDS/IPS провідних світових виробників.		http://dl.dut.edu.ua/course/view.php?id=1595	http://dl.dut.edu.ua/course/view.php?id=1595
	Практичне заняття 5	Тема: Дослідження стійкості парольного захисту програмного забезпечення.		1. Brute force and methods of counteraction. 2. Критерії стійкості парольного захисту.	http://dl.dut.edu.ua/course/view.php?id=1595	http://dl.dut.edu.ua/course/view.php?id=1595
	Практичне заняття 6	Тема: Операційна система. Виявлення уразливостей операційних систем Windows/UNIX.		Реалізувати основні методи захисту ОС від ШПЗ.	http://dl.dut.edu.ua/course/view.php?id=1595	http://dl.dut.edu.ua/course/view.php?id=1595
	Лабораторне заняття 4	Тема: Дослідження евристичного, поведінкового, сигнатурного аналізу та налагодження параметрів безпеки антивірусних програм (AVP).		Уміти характеризувати методи, заходи, функції та застосовувати можливості сучасних AVP.	http://dl.dut.edu.ua/course/view.php?id=1595	http://dl.dut.edu.ua/course/view.php?id=1595
	Лабораторне заняття 5	Тема: Адміністрування засобів антивірусного захисту та визначення політик і груп клієнтів на прикладі ESET/McAfee vendor systems.		1. Уміти реалізувати методи і засоби захисту програм від руйнуючих програмних засобів на прикладі продуктів ESET/McAfee vendor systems. 2. Використання систем software monitoring.. 3. Обґрунтовувати ефективні методи протидії від ШПЗ.	http://dl.dut.edu.ua/course/view.php?id=1595	http://dl.dut.edu.ua/course/view.php?id=1595

	Лабораторне заняття 6	Тема: Оцінка ефективності засобів захисту від програм Keyloggers.		1. Обґрунтовувати раціональні шляхи і типові методи та засоби протидії Keyloggers. 2. Налаштування параметрів функціонування antikeylogger monitor та antikeylogger scanner.	http://dl.dut.edu.ua/course/view.php?id=1595	http://dl.dut.edu.ua/course/view.php?id=1595
	Лабораторне заняття 7	Тема: Основні ознаки присутності ШПЗ та методи по усуненню наслідків заражень і несанкціонованих атак в ІТС.		1. Виявляти Computer Virus, Trojan-horse та інші malicious software в ОС на прикладі ESET/McAfee /AVG vendor systems. 2. Уміти виконувати захист файлів PC real-time protection of media, documents, HIPS, ANTI-STEALS, etc.	http://dl.dut.edu.ua/course/view.php?id=1595	http://dl.dut.edu.ua/course/view.php?id=1595
	Лабораторне заняття 8	Тема: Дослідження параметрів безпеки сучасних засобів захисту ІТС від розповсюдження Spam. Основи адміністрування ESET Endpoint Security.		1. Реалізувати типову систему ЗІ від розповсюдження Spam. 2. Проводити налаштування mail client configurations та scanning modules (IMAP/POP3/POP3S). 3. Використовувати модулі сканування HTTP/HTTPS.	http://dl.dut.edu.ua/course/view.php?id=1595	http://dl.dut.edu.ua/course/view.php?id=1595
	Лабораторне заняття 9	Тема: Захист інформації в ІТС організації. Основи адміністрування ESET Endpoint Security.		1. Проводити налаштування захисту system IDS від network attacks. 2. Проводити налаштування контролю вхідного і вихідного Fairwall network traffic of the system.	http://dl.dut.edu.ua/course/view.php?id=1595	http://dl.dut.edu.ua/course/view.php?id=1595

8. Мова вивчення освітньої компоненти

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

Українська, англійська

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

Бурячок В.Л. Інформаційний та кіберпростори: проблеми безпеки, методи та засоби боротьби [Підручник] / В.Л. Бурячок, Г.М. Гулак, В.Б. Толубко. – К.: ТОВ «СІК ГРУП Україна», 2015. – 449 с.

Бурячок В. Л. Інформаційний та кіберпростори: проблеми безпеки, методи та засоби боротьби. [Посібник]. / В. Л. Бурячок, С.В.Толюпа, В.В.Семко, Л.В.Бурячок, П.М.Складанний Н.В. Лукова-Чуйко/ – К. : ДУТ - КНУ, 2016. – 178 с.

Бурячок В. Л., Толубко В.Б., Хорошко В. О., Толюпа С.В. Інформаційна та кібербезпека: соціотехнічний аспект. [Підручник]. / В. Л. Бурячок, В.Б. Толубко, В. О. Хорошко, С.В. Толюпа /. За заг. ред. докт. техн. наук, проф. В.Б. Толубко. – К. : ДУТ, 2015. – 288 с. ISBN 978–966–2970–86–9
Waschke Marvin. Personal Cybersecurity: How to Avoid and Recover from Cybercrime. Personal Cybersecurity, Apress, 2017. – 240 p. – ISIN 978-1484224298.
Michael D. Hardware (ed.) How To Keep Your Personal Computer Running Like New Indefinitely! Windows & Apple Computers. Publisher: Michael D. Hardware, 2016. – 135 p. – ASIN: B01CUOPZRQ. – Kindle Edition
10. Методи оцінювання, підсумкові звітності за освітньою компонентою
(заліки, екзамени, курсові проекти, тестування)
залік
11. Матеріально-технічне забезпечення освітньої компоненти
Лабораторія 419, 420. ПК.

Виконано ст. викладачем Хмелевським Р.М.