

СИЛАБУС ДИСЦИПЛІНИ
«ОСНОВИ ЗАХИСТУ ІНФОРМАЦІЇ»

Рівень вищої освіти	**перший (бакалаврський)**
Спеціальність	**121 Інженерія програмного забезпечення**
Освітньо-професійна програма	**Інженерія програмного забезпечення**
Рік навчання	**3**
Семестр	**6**
Форма навчання	**денна**
Кількість кредитів ЄКТС	**5**
Мова викладання	**українська**

Лектор дисципліни

К.е.н. Віталій ВОРОБЙОВ

ОПИС ДИСЦИПЛІНИ

Курс «Основи захисту інформації» є важливою складовою навчального плану для студентів, які вивчають комп'ютерні науки, кібербезпеку та інформаційні технології. Головна мета цього курсу полягає в тому, щоб надати студентам знання та навички, необхідні для забезпечення безпеки інформаційних систем та захисту даних від різних загроз.

Студенти цього курсу вивчають основні принципи захисту інформації, включаючи концепції конфіденційності, цілісності та доступності даних, а також методи захисту інформаційних систем. Вони знайомляться з різними типами загроз та вразливостей, криптографічними методами захисту, управлінням доступом, безпекою мереж, а також політиками та процедурами забезпечення інформаційної безпеки.

СТРУКТУРА ДИЦИПЛІНИ

Тема	Години (лекції/ семінарські)	Результати навчання	Завдання	Оцінювання
6 семестр				
Тема 1 Введення в інформаційну безпеку	4/4	Студенти знатимуть: Основні поняття та визначення в галузі інформаційної безпеки. - Загрози і вразливості інформаційних систем. - Основні принципи захисту інформації. - Законодавчі аспекти інформаційної безпеки.	Питання, тести, виконання самостійної роботи	5

Тема 2. Криптографія і захист даних.	4/4	Студенти вмітимуть:Використовувати основні методи шифрування і цифрові підписи. Розуміти різницю між симетричним і асиметричним шифруванням. Застосовувати криптографічні методи для захисту даних в мережах.	Питання, тести, виконання самостійної роботи, методичні завдання.	5
Тема 3. Мережева безпека.	4/4	Студенти оволодіють основними принципами і методами захисту комп'ютерних мереж від зовнішніх атак.	Питання, тести, виконання самостійної роботи, методичні завдання.	5
Тема 4. Захист веб-додатків.	4/4	Вмітимуть: Налаштовувати і використовувати засоби мережевої безпеки, такі як firewalls і VPN. Розпізнавати і аналізувати мережеві атаки. Застосовувати методи захисту Wi-Fi мереж і мережевих пристроїв.	Питання, тести, виконання самостійної роботи, методичні завдання.	5
Тема 5. Управління ідентичністю і доступом.	4/4	Студенти зможуть визначати загрози для веб-додатків і застосовувати засоби захисту, такі як валідація введення та захист сесій. Розробляти веб-додатки з врахуванням принципів безпеки.	Питання, тести, виконання самостійної роботи, методичні завдання.	5
Тема 6. Аналіз загроз і відповіді на інциденти.	4/4	Вмітимуть виконувати виявлення та аналіз загроз інформаційній безпеці. Розробляти і виконувати плани відповіді на інциденти. Проводити тестування планів відповіді на інциденти.	Питання, тести, виконання самостійної роботи, методичні завдання.	5
Тема 7 Правові аспекти інформаційної безпеки.	4/4	Студенти засвоять основні правові аспекти, пов'язані з інформаційною безпекою і захистом даних.	Питання, тести, виконання самостійної роботи, методичні завдання.	5
Тема 8 Культура інформаційної безпеки.	4/4	Навчаться пропагувати культуру інформаційної безпеки серед співробітників і користувачів для запобігання внутрішнім загрозам	Питання, тести, виконання самостійної роботи	5
Всього балів за поточний контроль				**40**
Екзаменаційна оцінка				**60**
Всього				**100**

ПРОГРАМНІ КОМПЕТЕНТНОСТІ ТА РЕЗУЛЬТАТИ НАВЧАННЯ ЗДОБУВАЧА ВИЩОЇ ОСВІТИ

Інтегральна компетентність	Здатність розв'язувати складні спеціалізовані завдання або практичні проблеми інженерії програмного забезпечення, що характеризуються комплексністю та невизначеністю умов, із застосуванням теорій та методів інформаційних технологій
Програмні компетентності вивчення дисципліни	**загальні:** ЗК02. Здатність застосовувати знання у практичних ситуаціях. ЗК06. Здатність до пошуку, оброблення та аналізу інформації з різних джерел. **фахові:** СК 06. Здатність аналізувати, вибирати і застосовувати методи і засоби для забезпечення інформаційної безпеки (в тому числі кібербезпеки). СК 07. Володіння знаннями про інформаційні моделі даних, здатність створювати програмне забезпечення для зберігання, видобування та опрацювання даних. СК 10. Здатність накопичувати, обробляти та систематизувати професійні знання щодо створення і супроводження програмного забезпечення та визнання важливості навчання протягом всього життя. СК 13. Здатність обґрунтовано обирати та освоювати інструментарій з розробки та супроводження програмного забезпечення.
Програмні результати навчання	ПР18. Знати та вміти застосовувати інформаційні технології обробки, зберігання та передачі даних. ПР21. Знати, аналізувати, вибирати, кваліфіковано застосовувати засоби забезпечення інформаційної безпеки (в тому числі кібербезпеки) і цілісності даних відповідно до розв'язуваних прикладних завдань та створюваних програмних систем.

ПОЛІТИКА ОЦІНЮВАННЯ

Політика щодо дедлайнів та перескладання	Роботи, які здаються із порушенням термінів без поважних причин, оцінюються на нижчу оцінку. Перескладання відбувається із дозволу лектора за наявності поважних причин (наприклад, лікарняний).
Політика щодо академічної доброчесності	Списування під час контрольних робіт та екзаменів заборонені (в т.ч. із використанням мобільних девайсів). Курсові роботи, реферати повинні мати коректні текстові посилання на використану літературу.
Політика щодо відвідування	Відвідування занять є обов'язковим. За об'єктивних причин (наприклад, хвороба, міжнародне стажування) навчання може відбуватись індивідуально.

ШКАЛА ОЦІНЮВАННЯ ЗНАНЬ СТУДЕНТІВ

Оцінка за національною шкалою	Сума балів за всі види навчальної діяльності	Оцінка ECTS
відмінно	90 – 100	A
добре	82 – 89	B
	74 – 81	C
задовільно	64 – 73	D
	60 – 63	E
незадовільно з можливістю повторного складання	35 – 59	FX

незадовільно з обов’язковим повторним вивченням дисципліни	0 – 34	F

ЛІТЕРАТУРА ТА ІНФОРМАЦІЙНІ ДЖЕРЕЛА

Основна література	1. Богуш Володимир, Бровко Володимир, Настрадін Володимир Основи кіберпростору, кібербезпеки та кіберзахисту, Ліра-К: 2021 р. 554с. 2. Богуш В.М., Бровко В.Д., Кобус О.С., В.Д. Козюра В.Д, Технічний захист інформації. Навчальний посібник. 2023 р. 508 с. 3. Остапов С.Е., Євсеєв С.П., Король О.Г.ТЕХНОЛОГІЇ ЗАХИСТУ ІНФОРМАЦІЇ. Видавництво Новий світ-2020 р., 500с. 4. Principles of Information Security" by Michael E. Whitman and Herbert J. Mattord 2020 (7th Edition). 5. Cryptography and Network Security: Principles and Practice" by William Stallings 2022 (8th Edition). 6. Computer Security: Principles and Practice" by William Stallings and Lawrie Brown 2021 (4th Edition) 752 pages.
Інформаційні ресурси	1. Офіційне інтернет-представництво Президента України. URL: http://www.president.gov.ua/. 2. Верховна Рада України. URL:_ http://www.rada.kiev.ua/.