СИЛАБУС НАВЧАЛЬНОЇ ДИСЦИПЛІНИ

БЕЗПЕКА РОЗРОБКИ ТА ПІДТРИМКИ ДОДАТКІВ

Галузь знань	12 Інформаційні технології
Шифр та назва спеціальності	125 Кібербезпека та захист інформації
Назва освітньо-професійної програми	Кібербезпека та захист інформації
Рівень вищої освіти	Перший (бакалаврський)
Факультет	Інформаційни технологій та кібербезпеки
Кафедра	Кібербезпеки та технічного захисту інформації
Статус навчальної дисципліни	ОК-20 ОПП «Кібербезпека та захист інформації»
Форма навчання	Денна

Викладачі

Басов Віктор Євгенович
basvic@bigmir.net

Старший викладач кафедри «Кібербезпеки та технічного захисту інформації»
Кандидат технічних наук за фахом 05.12.02 – Телекомунікаційні системи та мережі

Загальна інформація про дисципліну

Анотація до дисципліни	Метою дисципліни «Безпека розробки та підтримки додатків» є забезпечення студентів базовими знаннями з проблем проектування та розробки додатків для систем обробки, зберігання та передавання інформації захищених від порушення властивостей конфіденційності, цілісності та доступності.

	. Навчання спрямовано на: 1) формування у здобувачів вищої освіти системного уявлення про застосування та розробку програмних систем для створення, зберігання та передавання інформації, а також чинників, що впливають на цей процес; 2) розвиток умінь з правильної експлуатації програмних систем, аналізу та розробки протоколів тестування, навичок оцінювання стійкості програмних систем до різноманітних видів атак на програмні ресурси та обладнання; 3) надання базових знань та первинних навичок до проектування як локальних, так і мережних програмних систем та протоколів взаємодії; 4) аналіз та розробка криптографічних протоколів для розподілу ключів в мережах зв'язку та протоколів розділення секрету.
Мета дисципліни	– формування системних знань та розвиток умінь щодо експлуатації, аналізу та розробки програмних систем з урахуванням вимог до захисту інформації при її створенні, зберіганні та передеванні через не захищене середовище..
Компетентності, формуванню яких сприяє дисципліна	ІК Здатність розв'язувати складні спеціалізовані задачі та практичні проблеми галузі забезпечення інформаційної безпеки та/або кібербезпеки, що характеризується комплексністю та неповною визначеністю умов. КЗ1. Здатність застосовувати знання у практичних ситуаціях КЗ2. Знання та розуміння предметної області та розуміння професії. КЗ4. Вміння виявляти, ставити та вирішувати проблеми за професійним спрямуванням КЗ5. Здатність до пошуку, оброблення та аналізу інформації КЗ7. 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 розвитку суспільства, техніки і технологій, використовувати різні види та форми рухової активності для активного відпочинку та ведення здорового способу життя. КФ2 Здатність до використання інформаційно комунікаційних технологій, сучасних методів і моделей інформаційної та/або кібербезпеки. КФ5. Здатність забезпечувати захист інформації, що обробляється в інформаційно-телекомунікаційних (автоматизованих) системах з метою реалізації встановленої політики інформаційної та/або кібербезпеки. КФ 6. Здатність відновлювати штатне функціонування інформаційних, інформаційно-телекомунікаційних (автоматизованих) систем після реалізації загроз, здійснення кібератак, збоїв та відмов різних класів та походження.. КФ9. Здатність здійснювати професійну діяльність на основі впровадження системи управління інформаційною та/або кібербезпекою. КФ 10. Здатність застосовувати методи та засоби криптографічного та технічного захисту інформації на об'єктах інформаційної діяльності.
Результати навчання	ПРН 1. Застосовувати знання державної та іноземних мов з метою забезпечення ефективності професійної комунікації. ПРН 26. Впроваджувати заходи та забезпечувати реалізацію процесів попередження отриманню несанкціонованого доступу і захисту інформаційних, інформаційно-телекомунікаційних (автоматизованих) систем на основі еталонної

	моделі взаємодії відкритих систем. ПРН 53. Вирішувати задачі аналізу програмного коду на наявність можливих загроз.
Обсяг дисципліни	Загальний обсяг дисципліни: 4 кредитів ЄКТС 120 годин). Для денної форми навчання: лекції – 18 годин, практичні заняття –18 години, лабораторні заняття – 18 годин, іспит – 2 годтни, самостійна робота – 64 годин.
Форма підсумкового контролю	Екзамен
Терміни викладання дисципліни	Дисципліна викладається у 5-му семестрі

Програма дисципліни

Тема 1.	**Введення до безпеки розробки програмного забезпечення (БРПЗ).** Традиційний процес випуску ПЗ та його слабкі місця, засоби захисту віртуального периметру та чому їх не достатньо, на яких етапах розробки ПЗ слід додавати засоби забезпечення безпеки.
Тема 2	**Управління базами даних.** Системи управління доступом до БД, моделі БД та особливості їх застосування, .мета та задачі проміжного ПЗ з точки зору безпеки, види захисту даних у БД.
Тема 3.	**Забезпечення цілісності даних.** Семантична, посилальна та логічна цілісність, що це таке та яким чином вони забезпечуються ПЗ БД. Інтелектуальний аналіз даних
Тема 4.	**Розробка програмних систем.** Керування розробкою, етапи життєвого циклу програмного забезпечення, управління ризиками
Тема 5.	**Методи розробки програмного забезпечення.** Перелік та характеристики методів розробки ПЗ, розробка прототипів, методологія безпечного проектування, методологія безпечної розробки, моделі зрілості процесів розробки ПЗ.
Тема 6	**Методологія розробки програмного забезпечення**. Об’єктно-орієнтоване програмування, моделювання даних, архітектура програмного забезпечення.
Тема 7	**Розподілені обчислення.** CORBA, EJB, Microsoft COM – як основні варіанти взаємодії у клієнт-серверній архітектурі. Розподілене обчислювальне середовище, експертні системи та штучний інтелект, нейронні мережі.
Тема 8	**Безпека WEB-додатків.** Види атак на web-додатки та захисні заходи.
Тема 9	**Мобільний код.** Java-апліти, Active-X. Види шкідливого ПЗ (віруси, черви, троянські програми, логічні бомби, бот-мережі,). Протидія шкідливому ПЗ.
Тема 10	**Керування патчами.** Методологія керування патчами, проблеми при встановленні патчів та найкращі практики керування патчами, види атак на web-додатки.

Список рекомендованих джерел

1. Басов В.Є. Практичні завдвння по курсу БРПЗ – методичний посібник на кафедрі.
2. Shon Harris, Fernando Mayumi. Praise for CISSP® All-in-One Exam Guide Copyright © 2019 by McGraw-Hill Education. - 1692
3. Smart Nigel. Cryptography: An Introduction, 3rd Edition.–A McGraw Hill Publication., 2003

Інформація про консультації

Кожного понеділка у лютому-травні 2024 року з 15^{00} до 16^{20} год., дистанційно. Ст. викл. Басов В. Є.

Загальна схема оцінювання

Сума балів за всі види навчальної діяльності	**Шкала ЄКТС**	**Оцінка за національною шкалою**		**Нарахування балів**	**Бали нараховуються таким чином:**
		для іспиту	**для заліку**		
90-100	A	Відмінно	Зараховано		***Оцінювання знань здобувачів вищої освіти здійснюється за 100-бальною шкалою*** і становить: за поточну успішність (участь у практичних заняттях, виконання практичних завдань та контрольних робіт) – до 60 балів, за результати екзамену – до 40 балів.
82-89	B	Добре			
74-81	C				
64-73	D	Задовільно			
60-63	E				
35-59	FX	Незадовільно з можливістю повторного складання	Не зараховано з можливістю повторного складання		
0-34	F	Незадовільно з обов'язковим повторним вивченням дисципліни	Не зараховано з обов'язковим повторним вивченням дисципліни		

Політика опанування дисципліни

Відвідування: Здобувачі вищої освіти самостійно планують відвідування лекційних занять, що проводяться в межах дисципліни. Присутність на практичних заняттях та контрольних заходах (екзамен/залік) є обов'язковою. При проведенні занять в онлайн режимі, присутність здобувача враховується у разі відкритого вікна.
Дотримання принципів академічної доброчесності: Підготовка усіх завдань, письмових робіт і т. ін., що виконуються в межах дисципліни, здійснюється здобувачем вищої освіти самостійно, на засадах академічної доброчесності. Викладач має право для перевірки робіт застосовувати програму **Unicheck.**
Умови зарахування пропущених занять:
Інші умови: Навчально-методичні матеріали дисципліни розміщені на платформі Moodle, за посиланням …….