



## СИЛАБУС НАВЧАЛЬНОЇ ДИСЦИПЛІНИ

### БЕЗПЕКА РОЗРОБКИ ТА ПІДТРИМКИ ДОДАТКІВ

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

#### Викладачі

Басов Віктор Євгенович  
[basvic@bigmir.net](mailto: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.

	<p>. Навчання спрямовано на:</p> <ol style="list-style-type: none"> <li>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;</li> <li>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;</li> <li>3) надання базових знань та первинних навичок до проектування як локальних, так і мережних програмних систем та протоколів взаємодії;</li> <li>4) аналіз та розробка криптографічних протоколів для розподілу ключів в мережах зв'язку та протоколів розділення секрету.</li> </ol>
<b>Мета дисципліни</b>	– формування системних знань та розвиток умінь щодо експлуатації, аналізу та розробки програмних систем з урахуванням вимог до захисту інформації при її створенні, зберіганні та передаванні через не захищене середовище..
<b>Компетентності, формуванню яких сприяє дисципліна</b>	<p>ІК Здатність розв'язувати складні спеціалізовані задачі та практичні проблеми галузі забезпечення інформаційної безпеки та/або кібербезпеки, що характеризується комплексністю та неповною визначеністю умов.</p> <p>КЗ1. Здатність застосовувати знання у практичних ситуаціях</p> <p>КЗ2. Знання та розуміння предметної області та розуміння професії.</p> <p>КЗ4. Вміння виявляти, ставити та вирішувати проблеми за професійним спрямуванням</p> <p>КЗ5. Здатність до пошуку, оброблення та аналізу інформації</p> <p>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.</p> <p>КФ2 Здатність до використання інформаційно комунікаційних технологій, сучасних методів і моделей інформаційної та/або кібербезпеки.</p> <p>КФ5. Здатність забезпечувати захист інформації, що обробляється в інформаційно-телекомунікаційних (автоматизованих) системах з метою реалізації встановленої політики інформаційної та/або кібербезпеки.</p> <p>КФ 6. Здатність відновлювати штатне функціонування інформаційних, інформаційно-телекомунікаційних (автоматизованих) систем після реалізації загроз, здійснення кібератак, збоїв та відмов різних класів та походження..</p> <p>КФ9. Здатність здійснювати професійну діяльність на основі впровадження системи управління інформаційною та/або кібербезпекою.</p> <p>КФ 10. Здатність застосовувати методи та засоби криптографічного та технічного захисту інформації на об'єктах інформаційної діяльності.</p>
<b>Результати навчання</b>	<p>ПРН 1. Застосовувати знання державної та іноземних мов з метою забезпечення ефективності професійної комунікації.</p> <p>ПРН 26. Впроваджувати заходи та забезпечувати реалізацію процесів попередження отриманню несанкціонованого</p>

	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.
<b>Обсяг дисципліни</b>	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.
<b>Форма підсумкового контролю</b>	Екзамен – 2 години
<b>Терміни викладання дисципліни</b>	Дисципліна викладається у 6-му семестрі

### Програма дисципліни

<b>Тема 1.</b>	<b>Введення до безпеки розробки програмного забезпечення (БРПЗ).</b> 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.
<b>Тема 2</b>	<b>Управління базами даних.</b> 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.
<b>Тема 3.</b>	<b>Забезпечення цілісності даних.</b> Семантична, посилальна та логічна цілісність, що це таке та яким чином вони забезпечуються ПЗ БД. Інтелектуальний аналіз даних
<b>Тема 4.</b>	<b>Розробка програмних систем.</b> Керування розробкою, етапи життєвого циклу програмного забезпечення, управління ризиками
<b>Тема 5.</b>	<b>Методи розробки програмного забезпечення.</b> Перелік та характеристики методів розробки ПЗ, розробка прототипів, методологія безпечного проектування, методологія безпечної розробки, моделі зрілості процесів розробки ПЗ.
<b>Тема 6</b>	<b>Методологія розробки програмного забезпечення.</b> Об'єктно-орієнтоване програмування, моделювання даних, архітектура програмного забезпечення.
<b>Тема 7</b>	<b>Розподілені обчислення.</b> CORBA, EJB, Microsoft COM – як основні варіанти взаємодії у клієнт-серверній архітектурі. Розподілене обчислювальне середовище, експертні системи та штучний інтелект, нейронні мережі.
<b>Тема 8</b>	<b>Безпека WEB-додатків.</b> Види атак на web-додатки та захисні заходи.
<b>Тема 9</b>	<b>Мобільний код.</b> Java-апліти, Active-X. Види шкідливого ПЗ (віруси, черви, троянські програми, логічні бомби, бот-мережі,). Протидія шкідливому ПЗ.
<b>Тема 10</b>	<b>Керування патчами.</b> 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 завдання 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 2023 року з 15<sup>00</sup> до 16<sup>20</sup> 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	Нарахування балів	<b>Оцінювання знань здобувачів вищої освіти здійснюється за 100-бальною шкалою і становить:</b> 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				
60-63	E	Задовільно			
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.