СИЛАБУС НАВЧАЛЬНОЇ ДИСЦИПЛІНИ «ТЕХНОЛОГІЇ БЕЗПЕЧНОГО ПРОГРАМУВАННЯ»

Ступінь вищої освіти – Бакалавр
Спеціальність 125 – КІБЕРБЕЗПЕКА
Освітня програма «Кібербезпека»
Рік навчання 3, семестр 5
Форма навчання денна
Кількість кредитів ЄКТС 4
Мова викладання українська

Лектор навчальної дисципліни	**Шкарупило Вадим Вікторович, к.т.н., доцент (портфоліо)** 
Контактна інформація лектора (e-mail)	**Кафедра комп'ютерних систем, мереж та кібербезпеки, корпус. 15, к. 207, тел. 5278724** **e-mail shkarupylo.vadym@nubip.edu.ua**
URL ЕНК на навчальному порталі НУБіП України	**ЕНК (1 семестр)** https://elearn.nubip.edu.ua/course/view.php?id=4664

ОПИС НАВЧАЛЬНОЇ ДИСЦИПЛІНИ

Завдання навчальної дисципліни «Технології безпечного програмування» – теоретична та практична підготовка здобувачів до розроблення та застосування сучасних технологій, підходів та практик здійснення безпечного програмування – засобів сприяння безпечності програмної складової комп'ютерних систем, призначених до функціонування в установах та на підприємствах, зокрема АПК.

Місце і роль дисципліни в системі підготовки фахівців відповідно до навчального плану. Дана навчальна дисципліна є теоретичною та практичною основою сукупності знань та вмінь, що формують профіль фахівця в області кібербезпеки.

Компетентності навчальної дисципліни:

Відповідно до освітньої програми підготовки фахівців за спеціальністю 125 «Кібербезпека» навчальна дисципліна забезпечує формування загальних і фахових компетентностей:

Загальні компетентності (ЗК):

ЗК 1. Здатність застосовувати знання у практичних ситуаціях.

ЗК 2. Знання та розуміння предметної області та розуміння професії.

ЗК 4. Вміння виявляти, ставити та вирішувати проблеми за професійним спрямуванням.

Спеціальні (фахові) компетентності (СК):

СК 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/або кібербезпеки.

СК 4. Здатність забезпечувати неперервність бізнесу згідно встановленої політики інформаційної та/або кібербезпеки.

СК 5. Здатність забезпечувати захист інформації, що обробляється в інформаційно-телекомунікаційних (автоматизованих) системах з метою реалізації встановленої політики інформаційної та/або кібербезпеки.

СК 6. Здатність відновлювати штатне функціонування інформаційних, інформаційно-телекомунікаційних (автоматизованих) систем після реалізації загроз, здійснення кібератак, збоїв та відмов різних класів та походження.

СК 7. Здатність впроваджувати та забезпечувати функціонування комплексних систем захисту інформації (комплекси нормативно-правових, організаційних та технічних засобів і методів, процедур, практичних прийомів та ін.).

СК 8. Здатність здійснювати процедури управління інцидентами, проводити розслідування, надавати їм оцінку.

СК 9. Здатність здійснювати професійну діяльність на основі впровадженої системи управління інформаційною та/або кібербезпекою.

Програмні результати навчання навчальної дисципліни:

ПРН 5. Адаптуватися в умовах частої зміни технологій професійної діяльності, прогнозувати кінцевий результат.

ПРН 6. Критично осмислювати основні теорії, принципи, методи і поняття у навчанні та професійній діяльності.

ПРН 7. Діяти на основі законодавчої та нормативно-правової бази України та вимог відповідних стандартів, у тому числі міжнародних в галузі інформаційної та /або кібербезпеки.

ПРН 8. Готувати пропозиції до нормативних актів щодо забезпечення інформаційної та /або кібербезпеки.

ПРН 9. Впроваджувати процеси, що базуються на національних та міжнародних стандартах, виявлення, ідентифікації, аналізу та реагування на інциденти інформаційної та/або кібербезпеки.

ПРН 25. Забезпечувати введення підзвітності системи управління доступом до електронних інформаційних ресурсів і процесів в інформаційних та інформаційно-телекомунікаційних (автоматизованих) системах з використанням журналів реєстрації подій, їх аналізу та встановлених процедур захисту.

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 28. Аналізувати та проводити оцінку ефективності та рівня захищеності ресурсів різних класів в інформаційних та інформаційно-телекомунікаційних (автоматизованих) системах в ході проведення випробувань згідно встановленої політики інформаційної та\або кібербезпеки.

ПРН 32. Вирішувати задачі управління процесами відновлення штатного функціонування інформаційно-телекомунікаційних систем з використанням процедур резервування згідно встановленої політики безпеки.

ПРН 34. Приймати участь у розробці та впровадженні стратегії інформаційної безпеки та/або кібербезпеки відповідно до цілей і завдань організації.

ПРН 39. Проводити атестацію (спираючись на облік та обстеження) режимних територій (зон), приміщень тощо в умовах додержання режиму секретності із фіксуванням результатів у відповідних документах.

ПРН 40. Інтерпретувати результати проведення спеціальних вимірювань з використанням технічних засобів, контролю характеристик ІТС відповідно до вимог нормативних документів системи технічного захисту інформації.

ПРН 41. Забезпечувати неперервність процесу ведення журналів реєстрації подій та інцидентів на основі автоматизованих процедур.

ПРН 42. Впроваджувати процеси виявлення, ідентифікації, аналізу та реагування на інциденти інформаційної, і/або кібербезпеки.

СТРУКТУРА НАВЧАЛЬНОЇ ДИСЦИПЛІНИ

Тема	Години (лекції/ лабораторні,)	Результати навчання	Завдання	Оцінювання
1 семестр				
Модуль 1. Шаблони проєктування, контейнери даних, контроль інваріантів.				
Базові принципи безпечного програмування.	**2/0**	Вміти слідувати на практиці фундаментальним засадам безпечного програмування.	Опитування.	**10**
Узагальнене програмування. Створення і використання шаблонних функцій.	**2/4**	Вміти створювати і використовувати шаблонні функції як засоби зниження збитковості та сприяння безпечності програмного коду.	Захист лабораторної роботи.	**10**
Узагальнене програмування. Створення і використання шаблонних класів.	**2/2**	Вміти створювати та застосовувати шаблонні класи як засоби безпечного виокремлення сімейств задіяних класів.	Захист лабораторної роботи.	**10**
Функтори як засоби сприяння безпечності програмного коду.	**2/2**	Вміти створювати і застосовувати функціональні об'єкти (функтори) у якості засобів безпечної реалізації функціоналу програмних потоків, а також у якості засобів сприяння безпечності операцій введення/виведення.	Захист лабораторної роботи.	**5**
Лямбда-вирази як засоби сприяння безпечності програмного коду.	**2/2**	Вміти створювати і застосовувати лямбда-вирази у якості засобів безпечної реалізації функціоналу програмних потоків, а також у якості засобів сприяння безпечності операцій введення/виведення.	Захист лабораторної роботи.	**5**
Сприяння безпечності за рахунок використання віртуального деструктора.	**2/2**	Вміти використовувати віртуальний деструктор у якості засобу безпечного вивільнення оперативної пам'яті.	Захист лабораторної роботи.	**20**
Безпечне використання шаблонів проєктування. Шаблон «Одинак».	**2/2**	Вміти реалізовувати і використовувати шаблон проєктування «Одинак» як запоруку безпечності з позиції контролю кількості екземплярів створюваних класів.	Захист лабораторної роботи.	**10**
Модульний контроль			Підсумковий тест в ЕНК	**30**
Модуль 2. Спеціалізовані технології безпечного програмування.				
Безпечне використання шаблонів проєктування. Мультипоточна реалізація шаблону «Одинак».	**2/2**	Вміти безпечно застосовувати шаблони шаблони проєктування у мультипоточному середовищі.	Захист лабораторної роботи. Опитування	**8** **2**
Безпечне використання шаблонів проєктування. Шаблон «Фабричний метод».	**2/2**	Вміти безпечно застосовувати шаблони шаблони проєктування у мультипоточному середовищі.	Захист лабораторної роботи.	**6**

			Опитування	**2**
Контроль інваріантів. Макрос «assert».	**2/2**	Вміти застосовувати макрос assert у якості засобу контролю значень виразів, зокрема для контролю інваріантів.	Захист лабораторної роботи. Опитування	**8** **2**
«Розумні» покажчики як засоби сприяння безпечності програмного коду.	**2/2**	Вміти створювати і використовувати «Розумні» покажчики у якості засобів сприяння безпечності на рівні виділення, використання та вивільнення оперативної пам'яті.	Захист лабораторної роботи. Опитування	**8** **2**
Застосування контейнерів даних як засобів досягнення безпечності динамічних виділення та вивільнення оперативної пам'яті.	**2/2**	Вміти застосовувати динамічні контейнери даних як засоби сприяння безпечності виділення і вивільнення оперативної пам'яті.	Захист лабораторної роботи. Опитування	**4** **2**
Узагальнені алгоритми, ітератори як засоби сприяння безпечності.	**2/2**	Вміти використовувати узагальнені алгоритми та ітератори у якості засобів сприяння безпечності при оперуванні наборами даних.	Захист лабораторної роботи. Опитування	**4** **2**
Модульні тести як засоби досягнення безпечності на рівні програмних модулів.	**2/2**	Вміти застосовувати модульні тести у якості засобів контролю розроблюваних програмних модулів.	Захист лабораторної роботи. Опитування	**8** **2**
Контроль нефункціональних характеристик у модульних тестах.	**2/2**	Вміти застосовувати модульні тести у якості засобів контролю нефункціональних характеристик розроблюваних програмних модулів.	Захист лабораторної роботи. Опитування	**8** **2**
Модульний контроль			Підсумковий тест в ЕНК	**30**
Всього				**70**
Екзамен			**Тест, написання програм**	**30**
Всього за 1 семестр				**100**
Курсова робота				**100**

ПОЛІТИКА ОЦІНЮВАННЯ

Політика щодо дедлайнів та перескладання:	Дедлайни визначені в ЕНК. Роботи, які здаються із порушенням термінів без поважних причин, оцінюються на нижчу оцінку. Перескладання модулів відбувається із дозволу лектора за наявності поважних причин (наприклад, лікарняний, стажування або відрядження).
Політика щодо академічної доброчесності:	Списування під час самостійних робіт, тестування та екзаменів заборонені (в т.ч. із використанням мобільних девайсів).
Політика щодо відвідування:	Відвідування занять є обов'язковим. За об'єктивних причин (наприклад, хвороба, міжнародне стажування) навчання може

	відбуватись індивідуально (в дистанційній on-line формі за погодженням із деканом факультету)

ШКАЛА ОЦІНЮВАННЯ ЗНАНЬ ЗДОБУВАЧІВ ВИЩОЇ ОСВІТИ

Рейтинг здобувача вищої освіти, бали	Оцінка національна за результати складання екзаменів заліків	
	Екзаменів	Заліків
90-100	Відмінно	зараховано
74-89	Добре	
60-73	Задовільно	
0-59	незадовільно	не зараховано

РЕКОМЕНДОВАНІ ДЖЕРЕЛА ІНФОРМАЦІЇ

1. ЕНК Технології безпечного програмування. URL: https://elearn.nubip.edu.ua/course/view.php?id=4664
2. What is safe programming and what steps need to be taken? URL: https://safeguardingsupporthub.org/webinars/what-safe-programming-and-what-steps-need-be-taken (дата звернення: 08.05.2022).
3. Standard Library Algorithms: Changes and Additions in C++17. URL: https://devblogs.microsoft.com/cppblog/standard-library-algorithms-changes-and-additions-in-c17/ (дата звернення: 08.05.2022).
4. Паттерни проектування. URL: https://refactoring.guru/uk/design-patterns (дата звернення: 08.05.2022).
5. C++ tutorial – functors (function objects). URL: https://www.bogotobogo.com/cplusplus/functors.php (дата звернення: 08.05.2022).
6. Multi-threaded programming terminology. URL: https://www.bogotobogo.com/cplusplus/multithreaded.php (дата звернення: 08.05.2022).
7. C++11/C++14 Thread 1. Creating threads. URL: https://www.bogotobogo.com/cplusplus/C11/1_C11_creating_thread.php (дата звернення: 08.05.2022).
8. ДСТУ ISO/IEC 2382:2017 (ISO/IEC 2382:2015, IDT) Інформаційні технології. Словник термінів.
9. ДСТУ EN 61508-1:2019 Функційна безпечність електричних, електронних, програмованих електронних систем, пов’язаних із безпекою. Частина 1. Загальні вимоги (EN 61508-1:2010, IDT; IEC 61508-1:2010, IDT). URL: http://online.budstandart.com/ua/catalog/doc-page?id_doc=84383 (дата звернення: 08.05.2022).