

**НАЦІОНАЛЬНИЙ УНІВЕРСИТЕТ БІОРЕСУРСІВ І  
ПРИРОДОКОРИСТУВАННЯ УКРАЇНИ**

Кафедра \_\_\_ комп'ютерних систем, мереж та кібербезпеки \_\_\_\_\_

**“ЗАТВЕРДЖУЮ”**

Декан факультету інформаційних технологій



проф. О.Г. Глазунова  
\_\_\_\_\_ 2023 р.

**СХВАЛЕНО**  
на засіданні кафедри  
комп'ютерних систем, мереж та кібербезпеки  
Протокол № 10 від «17» травня 2023 р.

*Касаткін Д.Ю.*  
Завідувач кафедри  
(доц. Касаткін Д.Ю.)

РОЗГЛЯНУТО  
Гарант ОП  
«Кібербезпека»

\_\_\_\_\_ Гарант ОП  
*Лахно В.А.* (проф. Лахно В.А.)

**РОБОЧА ПРОГРАМА НАВЧАЛЬНОЇ ДИСЦИПЛІНИ  
“Технології безпечного програмування”**

спеціальність \_\_\_\_\_ 125 – «Кібербезпека» \_\_\_\_\_

освітня програма \_\_\_\_\_ «Кібербезпека» \_\_\_\_\_

Факультет (ННІ) \_\_\_\_\_ інформаційних технологій \_\_\_\_\_

Розробники: \_\_\_\_\_ доцент, к.т.н., доцент Шкарупило В.В. \_\_\_\_\_

## 1. Опис навчальної дисципліни.

Технології безпечного програмування  
(назва)

<b>Галузь знань, напрям підготовки, спеціальність, освітньо-кваліфікаційний рівень</b>		
Галузь знань	Інформаційні технології	
Спеціальність	125 – «Кібербезпека»	
Освітньо-кваліфікаційний рівень	бакалавр	
<b>Характеристика навчальної дисципліни</b>		
Вид	Обов'язкова	
Загальна кількість годин	120	
Кількість кредитів ECTS	4	
Кількість змістових модулів	2	
Курсовий проект (робота) (якщо є в робочому навчальному плані)	30	
Форма контролю	Іспит	
<b>Показники навчальної дисципліни для денної та заочної форм навчання</b>		
	денна форма навчання	заочна форма навчання
Рік підготовки (курс)	2023-2024 (3)	-
Семестр	5	-
Лекційні заняття	30 год.	-
Практичні, семінарські заняття	-	-
Лабораторні заняття	30 год.	-
Самостійна робота	60 год.	-
Індивідуальні завдання	-	-
Кількість тижневих годин для денної форми навчання: аудиторних	4	

## 2. Мета, завдання та компетентності навчальної дисципліни.

**Мета** – набуття здобувачами знань та вмінь застосування сучасних технологій, підходів та практик, орієнтованих на досягнення безпечності програмування. Поняття безпечності при цьому адресується у контексті передбачуваності функціонування розробленої комп'ютерної системи.

**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.

**Вимоги щодо знань і вмінь, набутих внаслідок вивчення дисципліни.**

Внаслідок вивчення дисципліни студенти повинні:

**знати** актуальні підходи та технології створення безпечного програмного коду, відповідні засоби, механізми сприяння безпечності програмного коду; аспекти безпечної реалізації шаблонів проектування, зокрема у мультипоточному середовищі виконання програми.

**вміти** створювати безпечні реалізації шаблонів проектування, використовувати віртуальні деструктори, «розумні» покажчики, макрос «assert», лямбда-вирази, функтори, контейнери даних, адаптери контейнерів, ітератори, модульні тести – у якості засобів сприяння безпечності результуючого програмного коду.

#### **Набуття компетентностей:**

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

#### **Загальні компетентності (КЗ):**

КЗ 1. Здатність застосовувати знання у практичних ситуаціях.

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

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

#### **Спеціальні (фахові, предметні) компетентності спеціальності (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 (ПРН):**

ПРН 5. Адаптуватися в умовах частотої 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.

### **3. Програма та структура навчальної дисципліни для:**

– повного терміну денної форми навчання.

#### **Змістовий модуль 1. Базові засоби досягнення безпечності програмного коду.**

##### **Тема лекційного заняття 1. Базові принципи безпечного програмування:**

- мета, завдання дисципліни;
- базові принципи безпечного програмування;
- модифікатор «auto», тип «size\_t».

##### **Тема лекційного заняття 2. Узагальнене програмування. Створення і використання шаблонних функцій:**

- призначення шаблонних функцій;

- приклади використання шаблонних функцій.

**Тема лекційного заняття 3. Узагальнене програмування. Створення і використання шаблонних класів:**

- призначення шаблонних класів;
- приклади використання шаблонних класів.

**Тема лекційного заняття 4. Функтори як засоби сприяння безпечності програмного коду:**

- призначення і використання функторів;
- приклад використання функторів.

**Тема лекційного заняття 5. Лямбда-вирази як засоби сприяння безпечності програмного коду:**

- призначення і використання лямбда-виразів;
- приклад використання лямбда-виразів.

**Тема лекційного заняття 6. Сприяння безпечності за рахунок використання віртуального деструктора:**

- призначення віртуального деструктора;
- приклад використання віртуального деструктора.

**Тема лекційного заняття 7. Безпечне використання шаблонів проєктування. Шаблон «Одинак»:**

- реалізація шаблону «Одинак»;
- досягнення безпечності за рахунок використання статичних методів, модифікатору «delete».

**Змістовий модуль 2. Розвинуті засоби досягнення безпечності програмного коду.**

**Тема лекційного заняття 8. Безпечне використання шаблонів проєктування. Мультипоточна реалізація шаблону «Одинак»:**

- мультипоточна реалізація шаблону «Одинак»;
- застосування м'ютексів як засобів досягнення безпечності за рахунок синхронізації.

**Тема лекційного заняття 9. Безпечне використання шаблонів проєктування. Шаблон «Фабричний метод»:**

- сприяння безпечності за рахунок використання переліків, віртуального деструктора, «розумних» покажчиків;
- сприяння безпечності за рахунок використання макросу «assert».

**Тема лекційного заняття 10. Контроль інваріантів. Макрос «assert»:**

- макрос «assert» як засіб контролю інваріантів;
- сценарії використання макросу «assert».

**Тема лекційного заняття 11. «Розумні» покажчики як засоби сприяння безпечності програмного коду:**

- призначення і застосування «розумних» покажчиків;
- приклади застосування «розумних» покажчиків.

**Тема лекційного заняття 12. Застосування контейнерів даних як засобів досягнення безпечності динамічних виділення та вивільнення оперативної пам'яті:**

- класичний підхід до виділення/вивільнення динамічної пам'яті при створенні багатовимірних масивів, зокрема подань графів;
- безпечна реалізація багатовимірних масивів, зокрема графів, на основі контейнерів даних.

**Тема лекційного заняття 13. Модульні тести як засоби досягнення безпечності на рівні програмних модулів:**

- призначення, створення і використання модульних тестів;
- приклади використання модульних тестів.

**Тема лекційного заняття 14. Узагальнені алгоритми, ітератори як засоби сприяння безпечності:**

- використання узагальнених алгоритмів, ітераторів як засобів досягнення безпечності на рівні оперування елементами динамічних масивів;
- безпечне введення/виведення даних;
- приклади використання.

**Тема лекційного заняття 15. Асоціативні контейнери, адаптери контейнерів:**

- призначення і використання асоціативних контейнерів, адаптерів контейнерів;
- приклади використання.

### Структура навчальної дисципліни

Назви змістових модулів і тем	Кількість годин											
	денна форма						Заочна форма					
	Усього	у тому числі					усього	у тому числі				
		л	п	лаб	інд	с.р.		л	п	лаб	інд	с.р.
1	2	3	4	5	6	7	8	9	10	11	12	13
<b>Змістовий модуль 1. Базові засоби досягнення безпечності програмного коду.</b>												
Тема 1. Базові принципи безпечного програмування.	6	2		0		4						
Тема 2. Узагальнене програмування. Створення і використання шаблонних функцій.	10	2		4		4						
Тема 3. Узагальнене програмування. Створення і використання шаблонних класів.	8	2		2		4						

Тема 4. Функтори як засоби сприяння безпечності програмного коду.	8	2	2	4						
Тема 5. Лямбда-вирази як засоби сприяння безпечності програмного коду.	8	2	2	4						
Тема 6. Сприяння безпечності за рахунок використання віртуального деструктора. Макрос assert.	8	2	2	4						
Тема 7. Безпечне використання шаблонів проєктування. Шаблон «Одинак».	8	2	2	4						
<b>Разом за змістовим модулем 1</b>	<b>56</b>	<b>14</b>	<b>14</b>	<b>28</b>						
<b>Змістовий модуль 2. Розвинуті засоби досягнення безпечності програмного коду.</b>										
Тема 8. Безпечне використання шаблонів проєктування. Мультипоточна реалізація шаблону «Одинак».	8	2	2	4						
Тема 9. Безпечне використання шаблонів проєктування. Шаблон «Фабричний метод».	8	2	2	4						
Тема 10. Контроль інваріантів. Макрос «assert».	8	2	2	4						
Тема 11. «Розумні» показчики як засоби сприяння безпечності програмного коду.	8	2	2	4						
Тема 12. Застосування контейнерів даних як засобів досягнення безпечності динамічних виділення та вивільнення оперативної пам'яті.	8	2	2	4						
Тема 13. Узагальнені алгоритми, ітератори як засоби сприяння безпечності.	8	2	2	4						
Тема 14. Модульні тести як засоби досягнення безпечності на рівні програмних модулів.	8	2	2	4						
Тема 15. Контроль нефункціональних характеристик у модульних тестах.	8	2	2	4						
<b>Разом за змістовим модулем 2</b>	<b>64</b>	<b>16</b>	<b>16</b>	<b>32</b>						
Курсовий проєкт (робота) (якщо є в робочому навчальному плані)	<b>30</b>									
<b>Усього годин за курс</b>	<b>150</b>	<b>30</b>	<b>30</b>	<b>60</b>						

#### 4. Теми лабораторних занять.

№ з/п	Назва теми	Кількість годин
1	Створення і застосування шаблонних класів і функцій.	5
2	Безпечне застосування шаблонів проєктування.	5
3	Безпечне використання контейнерів даних.	5
4	Застосування «розумних» показчиків.	5

5	Застосування реалізацій алгоритмів стандартної бібліотеки.	5
6	Застосування модульних тестів.	5
	<b>Разом за семестр</b>	<b>30</b>
	<b>Разом</b>	<b>30</b>

## 5. Теми самостійної роботи.

№ з/п	Назва теми	Кількість годин
1	Базові принципи безпечного програмування. Шаблонізація як механізм уніфікації програмного коду.	4
2	Шаблонні функції як альтернатива перевантаженню функцій. Порівняльний аналіз.	4
3	Шаблонні класи як засоби узагальнення користувацьких типів.	4
4	Застосування функторів у якості засобів реалізації функціоналу програмних потоків.	4
5	Застосування лямбда-виразів у якості засобів реалізації функціоналу програмних потоків.	4
6	Ключове слово <code>auto</code> і тип <code>size_t</code> як засоби сприяння безпечності з позиції передбачуваності роботи відповідного програмного коду.	4
7	Шаблон проектування «Одинак» як представник сімейства породжуючих шаблонів.	4
8	Засоби синхронізації (м'ютекси) як механізми досягнення безпечності за мультипоточної реалізації шаблону проектування «Одинак».	4
9	Механізм забезпечення динамічного поліморфізму згідно шаблону проектування «Фабричний метод».	4
10	Шляхи забезпечення контролю результатів обчислень на основі макросу <code>assert</code> .	4
11	Розумні покажчики. Порівняльний аналіз та сценарії застосування.	4
12	Асоціативний список як динамічний контейнер даних, що сприяє безпечності з позиції уникнення дублювань елементів.	4
13	Аспекти застосування ітераторів із використанням ключового слова <code>auto</code> .	4
14	Параметризоване модульне тестування. Аспекти використання.	4
15	Модульне тестування у пакетному режимі.	4
	<b>Разом</b>	<b>60</b>

## 6. Зразки контрольних питань, тестів для визначення рівня засвоєння знань студентами.

- Простір імен як засіб досягнення безпечності програмного коду шляхом інкапсуляції.
- Шаблонні функції і класи як засоби досягнення безпечності програмного коду шляхом уніфікації.
- Методи та засоби стандартної бібліотеки шаблонів STL.
- Узагальнені алгоритми.
- Функціональні об'єкти.
- Лямбда-вирази.
- Контейнери і адаптери контейнерів.
- Множини і множини з дублюванням.



9. Словники і словники з дублюванням.
10. Списки і двонапрямлені черги.
11. Вектори векторів.
12. Асоціативні контейнери. Словники.
13. Асоціативні контейнери. Словники з дублікатами.
14. Адаптери контейнерів. Стеки.
15. Адаптери контейнерів. Черги.
16. Адаптери контейнерів. Черги з пріоритетами.
17. Ітератори. Використання ітераторів.
18. Реалізації алгоритмів стандартної бібліотеки C++ як засоби сприяння безпеці програмування – з позиції адаптації вже перевірених напрацювань.
19. Контроль інваріантів як механізм сприяння безпеці.
20. Контроль часових витрат на роботу функції (методу класу) як інструмент безпечного програмування.

## **7. Методи навчання.**

Під час викладання курсу використовуються наступні методи навчання:

- розповідь – для оповідної, описової форми розкриття навчального матеріалу;
- пояснення – для розкриття сутності певного явища, закону, процесу;
- бесіда – для усвідомлення, за допомогою діалогу, нових явищ, понять;
- ілюстрація – для розкриття предметів і процесів через їх символічне зображення (рисунок, схеми, графіки);
- лабораторна робота – для використання набутих знань при виконанні лабораторних завдань;
- аналітичний метод – для мисленнєвого або практичного розкладу цілого на частини з метою вивчення їх суттєвих ознак;
- проблемний виклад матеріалу – для створення проблемної ситуації.

## **8. Форми контролю.**

Наприкінці кожного змістовного модуля проводиться контрольна робота.

Перший змістовий модуль – захист п'яти лабораторних робіт, усне опитування, контрольна робота – тест.

Другий змістовий модуль – захист п'яти лабораторних робіт, усне опитування, контрольна робота – тест, екзамен.

## **9. Розподіл балів, які отримують студенти.**

Оцінювання знань студента відбувається за 100-бальною шкалою і переводиться в національні оцінки згідно з табл. 1 «ПОЛОЖЕННЯ про екзамен та заліки у НУБіП України» (наказ про уведення в дію від «26» квітня 2023 р. протокол № 10):

Рейтинг студента, бали	Оцінка національна за результати складання	
	екзаменів	заліків

90-100	Відмінно	Зараховано
74-89	Добре	
60-73	Задовільно	
0-59	Незадовільно	Не зараховано

Для визначення рейтингу студента (слухача) із засвоєння дисципліни  $R_{\text{дис}}$  (до 100 балів) одержаний рейтинг з атестації (до 30 балів) додається до рейтингу студента (слухача) з навчальної роботи  $R_{\text{НР}}$  (до 70 балів):  $R_{\text{дис}} = R_{\text{НР}} + R_{\text{ат}}$ .

Оцінка виконання та захисту лабораторних робіт за кожний модуль здійснюється у наступній відповідності:

№ лабораторної роботи	Кількість балів	Загальна кількість балів
<b>1 модуль</b>		
Лабораторна робота № 1	20	70
Лабораторна робота № 2	20	
Лабораторна робота № 3	20	
Самостійна робота	10	30
Модульна контрольна		
<b>2 модуль</b>		
Лабораторна робота № 4	20	70
Лабораторна робота № 5	20	
Лабораторна робота № 6	20	
Самостійна робота	10	30
Модульна контрольна		

## 10. Навчально-методичне забезпечення.

1. Методичні вказівки до лабораторних робіт з дисципліни "Технології безпечного програмування" для студентів спеціальності 125 "Кібербезпека" всіх форм навчання / Укл.: В.В. Шкарупило. – Київ: НУБіП, 2022. (прийнято до друку).

2. Електронний навчальний курс на платформі Moodle, що вміщує повне методичне забезпечення включаючи презентації до лекцій, методичні вказівки до виконання лабораторних робіт тощо. URL: <https://elearn.nubip.edu.ua/course/view.php?id=4664>

## 11. Рекомендовані джерела інформації.

### Базові:

1. Williams A. C++ concurrency in action: practical multithreading. NY: Manning Publications Co., 2012. 530 p.

2. Семеренко В.П. Програмування мовами C та C++ в середовищі Windows: навч. посіб. Вінниця : УНІВЕРСУМ – Вінниця, 2003. 128 с.

### Допоміжні:

1. 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).
2. 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).
3. Паттерни проектування. URL: <https://refactoring.guru/uk/design-patterns> (дата звернення: 08.05.2022).
4. C++ tutorial – functors (function objects). URL: <https://www.bogotobogo.com/cplusplus/functors.php> (дата звернення: 08.05.2022).
5. Multi-threaded programming terminology. URL: <https://www.bogotobogo.com/cplusplus/multithreaded.php> (дата звернення: 08.05.2022).
6. C++11/C++14 Thread 1. Creating threads. URL: [https://www.bogotobogo.com/cplusplus/C11/1\\_C11\\_creating\\_thread.php](https://www.bogotobogo.com/cplusplus/C11/1_C11_creating_thread.php) (дата звернення: 08.05.2022).
7. ДСТУ ISO/IEC 2382:2017 (ISO/IEC 2382:2015, IDT) Інформаційні технології. Словник термінів.
8. 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](http://online.budstandart.com/ua/catalog/doc-page?id_doc=84383) (дата звернення: 08.05.2022).