

Міністерство освіти і науки України
Національний аерокосмічний університет
«Харківський авіаційний інститут»

Кафедра комп'ютерних систем, мереж і кібербезпеки (№ 503)

ЗАТВЕРДЖУЮ

Гарант освітньої програми


(підпис)

Олег ІЛЛЯШЕНКО
ім'я та ПРІЗВИЩЕ)

« 29 » серпня 2025 р.

**СИЛАБУС *ОБОВ'ЯЗКОВОЇ*
НАВЧАЛЬНОЇ ДИСЦИПЛІНИ**

Технології безпечного програмування (Курсовий проект (КП))
(назва навчальної дисципліни)

Галузь знань: 12 «Інформаційні технології»
(шифр і найменування галузі знань)

Спеціальність: 125 «Кібербезпека та захист інформації»
(код і найменування спеціальності)

Освітня програма: «Безпека інформаційних і комунікаційних систем»
(найменування освітньої програми)

Рівень вищої освіти: перший (бакалаврський)

Силабус введено в дію з 01.09.2025 року

Харків 2025 рік

Розробник: Здоровець Ю.В, ст.викладач _____
(прізвище та ініціали, посада, науковий ступінь та вчене звання) (підпис)

Силабус розглянуто на засіданні кафедри _____
комп'ютерних систем, мереж і кібербезпеки
(назва кафедри)

Протокол № 1 від « 29 » 08 2025 р.

Завідувач кафедри Д.Т.Н., професор _____ Вячеслав ХАРЧЕНКО
(науковий ступінь та вчене звання) (підпис) (ім'я та ПРІЗВИЩЕ)

Погоджено з представником здобувачів освіти:

_____ Ілля МІЦИК
(підпис) (ім'я та ПРІЗВИЩЕ)

1. Загальна інформація про викладача



ПІБ: *Здоровець Юлія Володимирівна*

Посада: *старший викладач кафедри комп'ютерних систем, мереж і кібербезпеки*

Науковий ступінь:

Вчене звання:

E-mail: j.zdorovets@csn.khai.edu

Перелік дисциплін, які викладає: *Технології Java, Технології безпечного програмування, Технології безпечного програмування (КП), Базу даних, Ознайомча практика*

Напрями наукових досліджень: *Java, алгоритми та методи обчислення, IoT, Робототехнічні системи та комплекси.*

2. Опис навчальної дисципліни

Форма здобуття освіти	<i>Денна, заочна</i>
Семестр	<i>4 семестр</i>
Мова викладання	<i>Українська</i>
Тип дисципліни	<i>Обов'язкова</i>
Обсяг дисципліни: кредити ЄКТС/ кількість годин	<i>денна: 2 кредити ЄКТС / 60 годин (24 аудиторних, з яких: практичні (семінарські) заняття – 24, СРЗ – 36); заочна: 2 кредити ЄКТС / 60 годин (24 аудиторних, з яких: практичні (семінарські) заняття – 24, СРЗ – 36)</i>
Види навчальної діяльності	<i>Практичні (семінарські) заняття Самостійна робота здобувача</i>
Види контролю	<i>Підсумковий контроль у вигляді диференційованого заліку</i>
Пререквізити	<i>Дисципліна базується на знаннях, отриманих під час вивчення дисциплін у циклі загальної і професійної підготовки, передбачених навчальним планом спеціальності, а саме: «Вища математика», «Іноземна мова», «Основи права», «Українська мова за професійним спрямуванням», «Дискретна математика», «Основи функціонування комп'ютерів», «Технології безпечного програмування», «Навчальна практика».</i>

3. Мета та завдання навчальної дисципліни, переліки компетентностей та очікуваних результатів навчання

Мета вивчення: оволодіння студентами сучасними методами, навичками, вміннями необхідними для розв'язання комплексу сучасних наукових і прикладних завдань з об'єктно-орієнтованого програмування, а також формування твердих практичних навичок щодо розроблення програмного забезпечення з використанням об'єктно-орієнтованого підходу.

Завдання: оволодіти практичними навичками та вмін'ям у сфері в області розробки алгоритмів, створення, трансляції та налагодження прикладних програм, застосування бібліотек та модулів для створення програмних забезпечення для вирішення задач аналізу та захисту інформаційних систем, що необхідно для професійної підготовки бакалаврів зі спеціальності «Кібербезпека та захист інформації».

Загальні компетентності:

Після закінчення цієї програми здобувач освіти буде здатен:

ЗК 1. Здатність застосовувати знання у практичних ситуаціях.

ЗК 2. Знання та розуміння предметної області та розуміння професійної діяльності.

ЗК 3. Здатність спілкуватися державною мовою як усно, так і письмово.

ЗК 4. Здатність спілкуватися іноземною мовою.

ЗК 5. Здатність вчитися і оволодівати сучасними знаннями.

Фахові компетентності спеціальності (ФК):

Після закінчення цієї програми здобувач освіти буде здатен:

СК 1. Здатність застосовувати законодавчу та нормативно-правову базу, а також державні і міжнародні вимоги, практики і стандарти у професійній діяльності.

СК 2. Здатність використовувати інформаційні технології, сучасні методи і моделі кібербезпеки та системи захисту інформації.

СК 10. Здатність виконувати моніторинг інформаційних процесів, аналізувати, виявляти, оцінювати можливі вразливості та загрози інформаційному простору й інформаційним ресурсам згідно з встановленою політикою інформаційної безпеки.

Програмні результати навчання:

ПРН 1. Вільно спілкуватися державною мовою усно та письмово при виконанні професійних обов'язків.

ПРН 2. Спілкуватися іноземною мовою з метою забезпечення ефективності професійної комунікації.

ПРН 4. Організовувати власну професійну діяльність, обирати і використовувати оптимальні методи та способи розв'язання складних

спеціалізованих задач і практичних проблем у професійній діяльності, оцінювати їхню ефективність.

ПРН 7. Застосовувати й адаптувати теорії інформації та кодування, математичної статистики, чисел, криптографії та стеганографії, оброблення і передачі сигналів тощо, принципи, методи, поняття кібербезпеки та захисту інформації у навчанні та професійній діяльності. ПРН 50. Забезпечувати функціонування програмних та програмно-апаратних комплексів виявлення вторгнень різних рівнів та класів (статистичних, сигнатурних, статистично-сигнатурних).

ПРН 9. Знати та застосовувати законодавство України та міжнародні вимоги, практики і стандарти з метою здійснення професійної діяльності в галузі кібербезпеки та захисту інформації.

ПРН12. Застосовувати методи та засоби захисту інформації в інформаційних та інформаційно-комунікаційних системах відповідно до встановленої політики інформаційної безпеки.

ПРН13. Впроваджувати, налаштовувати, супроводжувати та підтримувати функціонування програмних і програмно-апаратних комплексів і систем кібербезпеки та захисту інформації як необхідні процедури для функціонування інформаційних й інформаційно-комунікаційних систем та\або інфраструктури організації в цілому.

ПРН14. Вирішувати задачі управління процесами відновлення штатного функціонування інформаційних та інформаційно-комунікаційних систем з використанням процедур резервування згідно встановленої політики безпеки і забезпечувати функціонування спеціального програмного забезпечення щодо захисту та відновлення інформації.

ПРН21. Виконувати впровадження, підтримку, аналіз ефективності систем виявлення несанкціонованого доступу, дій з інформацією в інформаційній системі, вразливостей, можливих загроз інформаційному простору й інформаційним ресурсам та використовувати комплекси захисту для забезпечення необхідного рівня захищеності інформації в інформаційних системах.

4. Зміст навчальної дисципліни

Модуль 1

Змістовний модуль 1

Тема 1. Постановка задачі на курсове проектування

Форма занять: ознайомча лекція.

Предмет, мета вивчення і задачі дисципліни. Структура та зміст дисципліни і методичні рекомендації щодо її вивчення. Місце дисципліни у навчальному процесі. Вимоги до знань та вмінь тих, хто навчається.

Самостійна робота здобувачів: опрацювання навчально-методичних матеріалів. Формування питань до викладача.

Тема 2. Основні вимоги до курсового проекту

Зміст та структура курсового проекту. Загальні положення. Основна частина. Список використаних джерел.

Практичне заняття 1: зміст та структура курсового проекту. Загальні положення. Основна частина: аналіз предметної області.

Практичне заняття 2: проведення аналітичного огляду існуючих методів та аналогічних рішень. Огляд літературних джерел та патентний пошук. Аналіз нормативних документів (НД ТЗІ, ISO/IEC 27001).

Самостійна робота здобувачів: опрацювання навчально-методичних матеріалів. Розробка структури курсового проекту. Складання плану дослідження. Визначення переліку джерел за темою проекту. Формування питань до викладача.

Змістовий модуль 2

Тема 3. Організація та проведення досліджень

Форма занять: ознайомча лекція.

Методологія дослідження: мета та предмет вивчення. Метод дослідження: поняття, його функція та ознаки. Типологія методів наукового дослідження. Методи, які використовуються на емпіричному рівні дослідження. Методи, які використовуються на теоретичному рівні дослідження.

Практичне заняття 3: формулювання мети, завдань та вимог до курсового проекту. Визначення критеріїв оцінки результатів. Розробка технічного завдання на програму.

Практичне завдання 4: вибір та обґрунтування архітектури програми. Проектування діаграми варіантів використання: опис ролей, опис прецедентів. Проектування діаграми послідовностей. Проектування графічного інтерфейсу.

Практичне заняття 5: реалізація обраної архітектури у вигляді діаграми пакетів (модулів); розробка діаграми класів: виявлення сутностей, зв'язків між ними, стислий опис кожної сутності; схема алгоритму, опис усіх методів: назва, призначення, сигнатура, призначення вхідних та вихідних параметрів.

Практичне заняття 6-7: розробка програмного коду. Документування програмного коду.

Самостійна робота здобувачів: опрацювання навчально-методичних матеріалів. Пошук та аналіз наукових публікацій за темою проекту. Складання бібліографічного списку. Порівняльний аналіз існуючих рішень та визначення їх недоліків. Проведення досліджень згідно індивідуального завдання. Деталізація завдань дослідження. Визначення очікуваних результатів та критеріїв їх оцінки. Обґрунтування наукової новизни та практичної цінності. Формування питань до викладача.

Змістовний модуль 3

Тема 4. Підготовка та захист курсового проекту

Оформлення курсового проекту. Загальні вимоги до оформлення. Ілюстрації, таблиці, формули. Оформлення списку використаних джерел. Порядок захисту курсового проекту. Оформлення презентації. Доповідь.

Практичне заняття 8: Тестування та верифікація програми. Підготовка тестових сценаріїв. Аналіз результатів тестування. Підготовка інструкції користувача.

Практичне заняття 9. Оформлення курсового проекту. Загальні вимоги до оформлення пояснювальної записки. Ілюстрації, таблиці, формули. Оформлення програмного коду. Оформлення списку використаних джерел за ДСТУ 8302:2015. Оформлення презентації. Структура та зміст доповіді. Підготовка відповідей на типові запитання.

Практичне заняття 10. Публічний захист курсового проекту. Доповідь з презентацією. Демонстрація програмного продукту.

Самостійна робота здобувачів: аналіз результатів роботи. Оформлення пояснювальної записки відповідно до вимог. Підготовка графічного матеріалу. Форматування списку джерел.

5. Індивідуальні завдання

Виконання курсового проекту. Теми курсового проекту обираються індивідуально кожному студенту.

6. Методи навчання

Проведення консультацій, практичних занять, конференції, а також самостійна робота студентів за матеріалами, опублікованими кафедрою (п.11, 12).

7. Методи контролю

Проведення поточного контролю з використанням системи управління курсами кафедри комп'ютерних систем, мереж і кібербезпеки, підсумковий контроль у вигляді заліку за результатами звітної конференції.

8. Критерії оцінювання та розподіл балів, які отримують здобувачі освіти

Таблиця 8.1 – Розподіл балів, які отримують здобувачі освіти

Складові навчальної роботи	Бали за одне заняття (завдання)	Кількість занять (завдань)	Сумарна кількість балів
Виконання індивідуального завдання	0...50	1	0...50
Доповідь під час захисту результатів виконання КП та відповіді на питання	0...20	1	0...20
Презентація з демонстрацією результатів роботи	0...20	1	0...20
Оформлення ПЗ у відповідності до вимог	0...10	1	0...10
Усього за семестр			0...100

Для отримання заліку необхідно пояснювальну записку (10 балів) з виконаним індивідуальним завданням (50 балів), підготувати презентацію (20 балів) та зробити доповідь за результатами виконаного завдання (20 балів). Під час складання заліку здобувач має можливість отримати максимум 100 балів.

Таблиця 8.2 – Шкали оцінювання: бальна та традиційна

Сума балів	Оцінка за традиційною шкалою	
	Іспит, диференційований залік	Залік
90 – 100	Відмінно	Зараховано
75 – 89	Добре	
60 – 74	Задовільно	
0 – 59	Незадовільно	Не зараховано

Критерії оцінювання роботи здобувач освіти протягом семестру

Задовільно (60-74) – здобувач має знання, навички та вміння для досягнення результатів навчання за програмою. Виконав усі етапи виконання курсового проекту на базовому рівні згідно затверджених вимог до курсових проектів і своєчасно представлений до захисту. Демонструє роботу програмного продукту. Оформив пояснювальну записку з незначними відхиленнями від вимог. Підготував презентацію та доповідь на базовому рівні. Відповідає на базові запитання щодо виконаного завдання.

Добре (75-89) – здобувач має знання, навички та вміння для досягнення результатів навчання за програмою. Виконав усі етапи курсового проектування на достатньому згідно затверджених вимог до курсових проектів і своєчасно представлений до захисту. Демонструє роботу програмного продукту. Обґрунтовує вибір методів для вирішення індивідуального завдання. Оформив пояснювальну записку згідно вимог. Підготував якісну презентацію та структуровану доповідь. Впевнено відповідає на більшість запитань.

Відмінно (90-100) – здобувач має глибокі знання, навички та вміння для досягнення результатів навчання за програмою на високому рівні. Виконав усі етапи курсового згідно затверджених вимог до курсових проектів і своєчасно представлений до захисту. Демонструє роботу програмного продукту. Має вміння логічно та аргументовано викладати матеріал, коректно використовувати статистичні, математичні та інші методи, проводити власні дослідження; володіння навичками узагальнення, формулювання висновків; вміння працювати з інформаційними джерелами; вміння ініціювати та обґрунтовувати інноваційні підходи до вирішення проблеми, що досліджується. Оформив пояснювальну записку з високою якістю графічних матеріалів. Підготував якісну презентацію. Демонструє глибоке розуміння теоретичних основ та практичних аспектів. Впевнено та вичерпно відповідає на всі запитання комісії, демонструє здатність до наукової дискусії.

9. Політика навчального курсу

Дотримання вимог академічної доброчесності здобувачами освіти під час вивчення навчальної дисципліни, у тому числі загальноприйнятих морально-етичних норм і правил поведінки, вимог академічної доброчесності, передбачених Положенням про академічну доброчесність Національного аерокосмічного університету «Харківський авіаційний інститут» (<https://khai.edu/files/uploads/polozenna/polozhennya-pro-akademichnu-dobrochesnist.pdf>). Очікується, що роботи здобувачів освіти будуть їх оригінальними дослідженнями або міркуваннями. Списування, втручання в роботу інших здобувачів освіти можуть бути розцінені як прояв академічної недоброчесності. Виявлення ознак академічної недоброчесності в письмовій роботі здобувача освіти є підставою для її незарахування викладачем незалежно від масштабів плагіату чи обману.

Вирішення конфліктів. Порядок і процедури врегулювання конфліктів, пов'язаних із корупційними діями, зіткненням інтересів, різними формами дискримінації та іншими ситуаціями, що можуть виникнути під час навчання, а також правила етичної поведінки регламентуються Кодексом етичної поведінки в Національному аерокосмічному університеті «Харківський авіаційний інститут» (<https://khai.edu/ua/university/normativna-baza/ustanovchi-dokumenti/kodeks-etichnoi-povedinki/>).

10. Методичне забезпечення

1. Сторінка дисципліни у системі дистанційного навчання «Ментор» [Ел. ресурс]. URL: <https://mentor.khai.edu/course/view.php?id=9534>
2. Система управління курсами кафедри комп'ютерних систем, мереж і кібербезпеки [Ел. ресурс]. – Режим доступу: <https://elearn.csn.khai.edu>

11. Рекомендована література

Базова

1. Java Platform Standard Edition 8 Documentation [Електронний ресурс]. – Режим доступу : <https://docs.oracle.com/javase/8/docs/>
2. Microsoft C++, C, and Assembler documentation [Електронний ресурс]. – Режим доступу : <https://docs.microsoft.com/en-us/cpp/?view=msvc-170>
3. Python 3.10.2 documentation [Електронний ресурс]. – Режим доступу : <https://docs.python.org/3/>
4. Важинський С. Е., Щербак Т. І. Методика та організація наукових досліджень навч. пос. Суми: СумДПУ ім. А. С. Макаренка, 2016. – 260 с.
5. Кібербезпека: сучасні технології захисту. Навчальний посібник для студентів вищих навчальних закладів. / С. Е. Остапов, С. П. Євсєєв, О.Г. Король. – Львів: «Новий Світ 2000», 2020. – 678 с

Допоміжна

1. Python Tutorial [Електронний ресурс]. – Режим доступу : <https://www.tutorialspoint.com/python/index.htm>
2. Java Tutorial [Електронний ресурс]. – Режим доступу : <https://www.tutorialspoint.com/java/index.htm> 6
3. C++ Tutorial [Електронний ресурс]. – Режим доступу : <https://www.tutorialspoint.com/cplusplus/index.htm>

12. Інформаційні ресурси

1. Державна служба спеціального зв'язку та захисту інформації України [Ел. ресурс]. URL: <http://www.dsszzi.gov.ua>
2. Кафедральний сайт Ел. ресурс]. URL: <http://www.csn.khai.edu>
3. Криптографічний захист інформації [Ел. ресурс]. URL: <http://www.bezpeka.com/ru/lib/spec/crypt.html>.
4. National Vulnerability Database [Ел. ресурс]. URL: <https://nvd.nist.gov/>
5. Кваліфікаційний центр інформаційних технологій та кібербезпеки ДержНДІ технологій кібербезпеки [Електронний ресурс]. – <http://dstszi.gov.ua/>