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

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

ЗАТВЕРДЖУЮ

Гарант освітньої програми
_____ Олег ІЛЛЯШЕНКО
(підпис) ім'я та ПРІЗВИЩЕ)

« 29 » серпня 2025 р.

СИЛАБУС *ОБОВ'ЯЗКОВОЇ* НАВЧАЛЬНОЇ ДИСЦИПЛІНИ

Ознайомча практика
(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)

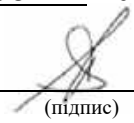
Силабус введено в дію з 01.09.2025 року

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), Бази даних, Ознайомча практика*

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

2. Опис навчальної дисципліни

Форма здобуття освіти	*Денна, заочна*
Семестр	4 семестр
Мова викладання	Українська
Тип дисципліни	*Обов'язкова*
Обсяг дисципліни: кредити ЄКТС/ кількість годин	*денна:* 3 кредити ЄКТС / 90 годин (СРЗ – 90) *заочна:* 3 кредити ЄКТС / 90 годин (СРЗ – 90)
Види навчальної діяльності	Самостійна робота здобувача
Види контролю	Підсумковий контроль у вигляді заліку
Пререквізити	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», «Системи технічного захисту інформації», «Теоретичні основи криптології»

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

Мета – надати студентам практичні навички створення, експлуатації та реінжинірингу комп'ютерних систем та мереж методами комп'ютерної інженерії.

Завдання: закріпити на практиці знання, вміння та навички розроблення програмних систем, а також:

– розглянути процес рецензування вихідного коду (Code Review);

– розглянути CI/CD парадигму розроблення сучасних програмних комплексів та систем;

– ознайомити студентів з існуючими системами контролю версій;

навчити студентів використовувати систему контролю версій Git в процесі навчання та під час виконання лабораторних/курсових/кваліфікаційних робіт.

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.

ЗК3. Здатність спілкуватися державною мовою як усно, так і письмово.

ЗК 4. Здатність спілкуватися іноземною мовою.

ЗК 5. Здатність вчитися і оволодівати сучасними знаннями.

Спеціальні (фахові предметні) компетентності спеціальності (СК):

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 9. Здатність застосовувати методи та засоби технічного захисту інформації на об'єктах інформаційної діяльності.

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.

Ррезультати навчання:

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

РН4. 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.

РН5. Аналізувати, аргументувати, приймати рішення при розв’язанні складних спеціалізованих задач і практичних завдань у професійній діяльності, які характеризуються комплексністю та неповною визначеністю умов, відповідати за прийняті рішення.

РН6. Адаптуватися до нових умов і технологій професійної діяльності, прогнозувати кінцевий результат.

РН7. 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.

РН9. Знати та застосовувати законодавство України та міжнародні вимоги, практики і стандарти з метою здійснення професійної діяльності в галузі кібербезпеки та захисту інформації.

РН10. Використовувати сучасні інформаційні технології, методи і моделі кібербезпеки та систем захисту інформації для здійснення професійної діяльності.

РН12. Застосовувати методи та засоби захисту інформації в інформаційних та інформаційно-комунікаційних системах відповідно до встановленої політики інформаційної безпеки.

4. Зміст навчальної дисципліни

Модуль 1

Змістовний модуль 1

Модуль 1.

Змістовний модуль 1.

Тема 1. Техніка безпеки і охорона праці на об'єкті практики

Форма занять: ознайомча лекція.

Проходження інструктажу з техніки безпеки і охорони праці, ознайомлення з правилами внутрішнього розпорядку. Ознайомлення з метою та програмою практики.

Тема 2. Постановка задачі на ознайомчу практику

Самостійна робота здобувачів

Вибір індивідуального завдання. Складання плану роботи. Визначення переліку джерел за темою роботи.

Змістовний модуль 2.

Тема 3. Робота над індивідуальним завданням

Самостійна робота здобувачів

Аналіз предметної області індивідуального завдання: огляд підходів, аналіз існуючих рішень, аналіз літератури та веб-джерел. Визначення об'єкта та

предмета дослідження на ознайомчі практиці. Вивчення нормативно-правової бази за темою дослідження.

Тема 4. Виконання індивідуального завдання.

Форма занять: самостійна робота здобувача освіти.

Вивчення наукових розробок в напрямку обраної теми. Проведення аналізу та досліджень згідно тематики індивідуального завдання. Виконання поставлених задач. Аналіз та верифікація отриманих результатів. Документування отриманих результатів.

Використання інструментальних засобів для генерації програмної документації. Оформлення звітів згідно з ДСТУ та іншими заданими вимогами.

Тема 5. Підготовка та оформлення звітних матеріалів.

Форма занять: самостійна робота здобувача освіти.

Узагальнення та систематизація матеріалу щодо проходження ознайомчої практики. Підготовка необхідної документації. Оформлення щоденнику з практики. Створення презентацій за тематикою індивідуального завдання. Підготовка до доповіді за результатами роботи.

Тема 6. Залік з ознайомчої практики

Форма занять:звітна конференція.

Звіт здобувачів освіти по результатам проходження практики. Підведення підсумків. складання заліку за результатами проходження ознайомчої практики.

5. Індивідуальні завдання

1. Аналіз біометричних систем контролю доступу.
2. Принципи побудови комплексу інженерно-технічних засобів системи охорони.
3. Аналіз систем сигналізації та контролю доступу.
4. Аналіз каналів витоку інформації.
5. Дослідження технічних засобів активного захисту мовної інформації в лініях зв'язку.
6. Аналіз закладних пристроїв (далі - ЗП) перехоплення мовної інформації.
7. Оцінка застосування мобільних пристроїв для перехоплення інформації.
8. Аналіз захисту від перехоплення інформації при передачі по телефонних каналах.
9. Завдання і структура системи охорони об'єкта, сучасні вимоги, що пред'являються до СО.
10. Дослідження придушення радіоканалів витоку інформації.
11. Аналіз засобів запобігання витоку інформації через ПЕМВН.

12. Оцінка ризиків інформаційної безпеки в безпроводних мережах стандарту IEEE 802.11.

13. Оцінка забезпечення безпеки інформаційних ресурсів в системах електронних платежів.

14. Оцінка захисту банківських транзакцій в системах інтернет-банкінгу.

15. Аналіз інформаційної безпеки в системах охоронного відеоспостереження.

16. Аналіз напрямків застосування штучного інтелекту в задачах кібербезпеки.

17. Система для генерування та аналізу криптографічних протоколів.

18. Дослідження сучасних методів проведення автентифікації користувачів в корпоративних інформаційно-телекомунікаційних системах та вироблення рекомендацій щодо підвищення їх ефективності.

19. Дослідження шляхів та вироблення рекомендацій щодо побудови інформаційних систем персональних даних в захищеному виконанні.

20. Дослідження шляхів забезпечення безпеки та вироблення рекомендацій щодо побудови системи захисту інформації WEB-порталу.

21. Оцінка ефективності розвідки у сфері інформаційної безпеки.

6. Методи навчання

Проведення консультацій, 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 практики та відповіді на питання	0…20	1	0…20
Презентація з демонстрацією результатів роботи	0…10	1	0…10
Оформлення щоденника практики	0…20	1	0…20
Усього за семестр			**0…100**

Для отримання заліку необхідно підготувати щоденник практики (20 балів) з виконаним індивідуальним завданням (50 балів), підготувати презентацію (10 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 ознайомчої практики на базовому рівні. Оформив щоденник практики 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 ознайомчої практики на

достатньому рівні. Обґрунтовує вибір методів захисту для вирішення індивідуального завдання. Оформив щоденник практики 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 ознайомчої практики на високому рівні. Вільно оперує термінологією в рамках індивідуального завдання. Самостійно аналізує сучасні рішення в межах індивідуального завдання, пропонує інноваційні рішення в рамках поставленого завдання. Оформив щоденник практики 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/assets/files/ polozhennya/polozhennya-pro-akademichnu-dobrochesn ist.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 недоброчестності. 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. Важинський С. Е., Щербак Т. І. Методика та організація наукових досліджень навч. пос. Суми: СумДПУ ім. А. С. Макаренка, 2016. – 260 с.
2. Кібербезпека: сучасні технології захисту. Навчальний посібник для студентів вищих навчальних закладів. / С. Е. Остапов, С. П. Євсеєв, О.Г. Король. – Львів: «Новий Світ2000», 2020. – 678 с
3. Криптологія: навч. посібник / М.Н. Курко, П.М. Лісовський, Ю.П. Лісовська. — К.: Видавничий дім «Кондор», 2020. — 248 с.
4. Клесов О.І., Елементарна теорія чисел та елементи криптографії, 2017, ТВіМС, Київ, 394 стор.
5. Клесов О.І., Елементарна теорія чисел та елементи криптографії, 2017, ТВіМС, Київ, 394 стор.
6. Матвієнко М. П., Розен В. П. Комп’ютерна схемотехніка. Навчальний посібник. – К.: Видавництво Ліра-К, 2020. – 192 с.

Допоміжна

1. Основи прикладної теорії цифрових автоматів: підручник / І. А. Дичка, В. П. Тарасенко, М. В. Онай ; КПІ ім. Ігоря Сікорського. – Київ: КПІ ім. Ігоря Сікорського, 2019. – 506 с.
2. Комп’ютерна схемотехніка: Навчальний посібник. – Луцьк: РРВ Луцького НТУ, 2016. – 236 с.
3. ДСТУ ISO/IEC 27001:2023 Інформаційна безпека, кібербезпека та захист конфіденційності. Системи керування інформаційною безпекою.
4. Богуш В. М., Богуш В. В., Бровко В. Д., Настрадін В. П. Основи кіберпростору, кібербезпеки та кіберзахисту / Ліра-К, 2021. – 554 с.

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/cript.html.
4. National Vulnerability Database [Ел. ресурс]. URL: https://nvd.nist.gov/