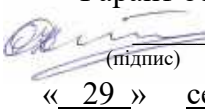
Міністерство освіти і науки України
Національний аерокосмічний університет
«Харківський авіаційний інститут»

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

ЗАТВЕРДЖУЮ
Гарант освітньої програми

О. Ілляшенко
(підпис) (ініціали та прізвище)
« 29 » серпня 2025 р..

СИЛАБУС ОБОВ'ЯЗКОВОЇ НАВЧАЛЬНОЇ ДИСЦИПЛІНИ

«Виробнича практика»
(назва навчальної дисципліни)

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

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

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

Рівень вищої освіти: перший (бакалаврський)

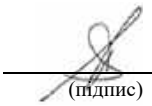
Силабус введено в дію з 01.09.2025 року

Харків – 2025 р.

Розробник: Лейченко К. М., доц. каф. 503, д-філ (PhD). 
(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: Лейченко Кирило Миколайович

Посада: доцент

Науковий ступінь: доктор філософії (PhD)

Вчене звання:

Перелік дисциплін, які викладає:

- Комп’ютерні мережі;
- Основи програмування;
- Технології Data Science;
- Виробнича практика;

Напрями наукових досліджень:
Прокладання та розміщення безпілотних інтелектуальних систем, моніторинг об’єктів критичної інфраструктури, великі дані.

Контактна інформація:
k.leychenko@csn.khai.edu

2. Опис навчальної дисципліни

Форма здобуття освіти	*Денна*
Семестр	6 семестр
Мова викладання	Українська
Тип дисципліни	*Обов'язкова*
Обсяг дисципліни: кредити ЄКТС/ кількість годин	*денна:* 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», «Дискретна математика», «Основи функціонування комп'ютерів», «Технології програмування», «Навчальна практика», «Ознайомча практика»
Кореквізити	Матеріал, засвоєний під час вивчення цієї дисципліни, є базою для дисциплін ОК33 «Кваліфікаційна робота бакалавра».

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

Мета – використовувати знання зі створення комп'ютерних систем та мереж методами комп'ютерної інженерії в практиці проектування комп'ютерних систем та мереж на виробництві.

Завдання: отримати навички та уміння при створенні комп'ютерних систем та мереж для обробки інформації та управління на реальних підприємствах.

Компетентності, які набуваються:

Загальні компетентності:

КЗ 1. Здатність застосовувати знання у практичних ситуаціях.

КЗ 2. Знання та розуміння предметної області і розуміння професійної діяльності.

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

КЗ 4. Здатність спілкуватися іноземною мовою.

КЗ 5. Здатність вчитися і оволодівати сучасними знаннями.

Фахові компетентності:

КФ 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.

КФ 3. Здатність до використання програмних та програмно-апаратних комплексів засобів захисту інформації в інформаційно-телекомунікаційних (автоматизованих) системах.

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

КФ 12. Здатність аналізувати, виявляти та оцінювати можливі загрози, уразливості та дестабілізуючі чинники інформаційному простору та інформаційним ресурсам згідно з встановленою політикою інформаційної та/або кібербезпеки.

Програмні результати навчання:

ПРН 1 Застосовувати знання державної та іноземних мов з метою забезпечення ефективності професійної комунікації.

ПРН 2 Організовувати власну професійну діяльність, обирати оптимальні методи та способи розв'язування складних спеціалізованих задач та практичних проблем у професійній діяльності, оцінювати їхню ефективність.

ПРН 3 Використовувати результати самостійного пошуку, аналізу та синтезу інформації з різних джерел для ефективного рішення спеціалізованих задач професійної діяльності.

ПРН 4 Аналізувати, аргументувати, приймати рішення при розв'язанні складних спеціалізованих задач та практичних проблем у професійній

діяльності, які характеризуються комплексністю та неповною визначеністю умов, відповідати за прийняті рішення.

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 11 Виконувати аналіз зв'язків між інформаційними процесами на віддалених обчислювальних системах.

ПРН 13 Аналізувати проекти інформаційно-телекомунікаційних систем базуючись на стандартизованих технологіях та протоколах передачі даних.

ПРН 15 Використовувати сучасне програмно-апаратне забезпечення інформаційно-комунікаційних технологій.

ПРН 19 Застосовувати теорії та методи захисту для забезпечення безпеки інформації в інформаційно-телекомунікаційних системах.

ПРН 22 Вирішувати задачі управління процедурами ідентифікації, автентифікації, авторизації процесів і користувачів в інформаційно-телекомунікаційних системах згідно встановленої політики інформаційної і\або кібербезпеки.

ПРН 31 Застосовувати теорії та методи захисту для забезпечення безпеки елементів інформаційно-телекомунікаційних систем.

ПРН 38 Інтерпретувати результати проведення спеціальних вимірювань з використанням технічних засобів, контролю характеристик інформаційно-телекомунікаційних систем відповідно до вимог нормативних документів системи технічного захисту інформації.

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

ПРН 47 Вирішувати задачі захисту інформації, що обробляється в інформаційно-телекомунікаційних системах з використанням сучасних методів та засобів криптографічного захисту інформації.

ПРН 50 Забезпечувати функціонування програмних та програмно-апаратних комплексів виявлення вторгнень різних рівнів та класів (статистичних, сигнатурних, статистично-сигнатурних).

ПРН 51 Підтримувати працездатність та забезпечувати конфігурування систем виявлення вторгнень в інформаційно-телекомунікаційних системах.

ПРН 54 Усвідомлювати цінності громадянського (вільного демократичного) суспільства та необхідність його сталого розвитку, верховенства права, прав і свобод людини і громадянина в Україні.

4. Зміст навчальної дисципліни

МОДУЛЬ 1

Змістовий модуль 1.

Тема 1. Вступ

Стисла анотація: Проходження інструктажу з техніки безпеки на початку практики. Ознайомлення з метою та програмою практики, отримання завдання.

Тема 2. Проектування і розроблення програмного забезпечення

Стисла анотація: Специфікація програмних вимог. Вибір інструментарію і розроблення технічного завдання для програмної реалізації завдання.

Тема 3. Тестування програмного забезпечення

Стисла анотація: Тестування програмного продукту з використанням сучасних підходів та інструментальних засобів.

Змістовний модуль 2

Тема 4. Документування програмного забезпечення

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

Тема 5. Презентація

Стисла анотація: Створення презентацій засобами PowerPoint. Підготовка та представлення доповіді.

5. Індивідуальні завдання

1. **Безпека програмного забезпечення на етапі розробки (SDL):**
   - Вивчення методологій SDL та їх застосування на практиці.
   - Розробка безпечного програмного забезпечення з урахуванням вимог SDL.
   - Автоматизація процесів SDL за допомогою сучасних інструментів.
2. **Криптографічні методи захисту інформації в програмному забезпеченні:**
   - Огляд сучасних криптографічних алгоритмів та їх застосування.
   - Реалізація криптографічного захисту даних у програмному забезпеченні.
   - Аналіз ефективності та безпеки використаних криптографічних методів.
3. **Безпека мобільних додатків:**
   - Дослідження особливостей безпеки мобільних платформ (Android, iOS).
   - Розробка безпечного мобільного додатку з урахуванням вимог платформи.
   - Аналіз безпеки розробленого додатку за допомогою спеціалізованих інструментів.
4. **Безпека десктопних додатків:**
   - Дослідження особливостей безпеки десктопних платформ (Unix, Windows).
   - Розробка безпечного десктопного додатку з урахуванням вимог платформи.
   - Аналіз безпеки розробленого додатку за допомогою спеціалізованих інструментів.
5. **Безпека інтернету речей (IoT):**
   - Вивчення проблем безпеки IoT-пристроїв та мереж.
   - Розробка безпечного IoT-рішення для конкретної задачі.
   - Аналіз безпеки розробленого рішення та його відповідності сучасним стандартам.
6. **Методи статичного та динамічного аналізу коду:**
   - Огляд інструментів для статичного та динамічного аналізу коду.
   - Застосування цих інструментів для пошуку вразливостей у програмному забезпеченні.
   - Порівняльний аналіз ефективності різних методів аналізу коду.
7. **Фаззінг та його застосування для пошуку вразливостей:**
   - Вивчення методів фаззингу та їх застосування на практиці.
   - Розробка власного фаззера для тестування конкретного програмного забезпечення.
   - Аналіз результатів фаззингу та виявлення вразливостей.
8. **Розробка безпечних API:**
   - Дослідження принципів безпечної розробки API.

- Розробка безпечного API для веб-додатку або мобільного додатку.
- Тестування безпеки розробленого API за допомогою спеціалізованих інструментів.

9. **Безпека операційних систем:**
    - Вивчення механізмів безпеки сучасних операційних систем.
    - Аналіз вразливостей операційних систем та методів їх захисту.
    - Розробка ПО для оцінки та генерування підвищення безпеки операційної системи.

6. Методи навчання

Проведення консультацій, звітної конференції, а також самостійна робота здобувачів за відповідними матеріалами.

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
Змістовний модуль 1			
Звіт	0…40	1	0…40
Тестові набори	0...15	1	0…15
Презентація	0...35	1	0…35
Модульний контроль	0…10	1	0…10
Усього за семестр			**0…100**

Для отримання заліку необхідно підготувати звіт (40 балів), описати тестові набори (15 балів), підготувати презентацію (35 балів) та виконати завдання з модульного контролю (10 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). Показати мінімум знань та умінь. Розробити тестові набори та підготовити звіт з розроблення програмного забезпечення. Знати можливості та основні положення роботи з мовою програмування С. Знати основи роботи з середовищем Microsoft Visual Studio. Знати основи роботи із засобом Microsoft PowerPoint. Уміти використовувати Microsoft Visual Studio та мову програмування С для вирішення практичних задач

Добре (75-89). Твердо знати мінімум. Розробити тестові набори, підготовити звіт з розроблення програмного забезпечення та презентацію виконаної роботи. Знати основи роботи з системою контроля версій Git. Знати ключові принципи структурного програмування. Знати базові структури даних. Уміти розробляти алгоритми та документувати їх у вигляді схем алгоритмів

Відмінно (90-100). Здати всі контрольні точки з оцінкою «відмінно». Виступити з презентацією виконаної роботи.

9. Політика навчального курсу

Дотримання вимог академічної доброчесності здобувачами освіти під час вивчення навчальної дисципліни. Під час вивчення навчальної дисципліни здобувані освіти мають дотримуватися 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-dobrochesnist.pdf). Очікується, що роботи здобувачів освіти будуть їх оригінальними дослідженнями або міркуваннями. Списування, втручання в роботу інших здобувачів освіти становлять, але не обмежують, приклади можливої академічної недоброчестності. Виявлення ознак академічної недоброчесності в письмовій роботі здобувана 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, сексуальними домаганнями, міжособистісними стосунками 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=1631.

11. Рекомендована література

Базова

1. Берко А.Ю., Верес О.М., Пасічник В.В. Системи баз даних та знань: підручник. / Видавництво: «Магнолія-2006», 2013. – 680 с.
2. Берко А.Ю., Верес О.М., Пасічник В.В. Системи баз даних та знань: навч.посібник. / Видавництво: «Магнолія-2006», 2008. – 456 с.
3. Журавський Ю.П., Полторак В.П. Теорія інформації та кодування: підручник. / К.: Вища школа, 2001. - 255 с.
4. ДСТУ 3008:2015. Інформація та документація. Звіти у сфері науки і техніки: Структура і правила оформлювання. – К.: ДП «УкрНДНЦ», 2016. – 26 с.

Допоміжна

1. В.Гребенніков. Нормативно-правове забезпечення інформаційної безпеки. Збірник лекцій.
2. Сальнікова І.І. PowerPoint для початківця. Навчальний посібник. – 112 с.

12. Інформаційні ресурси

1. Modern C [Ел. ресурс]. – Режим доступу: http://icube-icps.unistra.fr/index.php/File:ModernC.pdf
2. Microsoft PowerPoint 2016: Step by step [Ел. ресурс]. – Режим доступу: https://ptgmedia.pearsoncmg.com/images/9780735697799/samplepages/9780735697799.pdf