Міністерство освіти і науки України
Національний аерокосмічний університет ім. М. Є. Жуковського
«Харківський авіаційний інститут»

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

ЗАТВЕРДЖУЮ

Гарант освітньої програми
_____ О.О. Ілляшенко
(підпис) (ініціали та прізвище)

« 31 » серпня 2023 р.

РОБОЧА ПРОГРАМА ОБОВ'ЯЗКОВОЇ НАВЧАЛЬНОЇ ДИСЦИПЛІНИ

Виробничаа практика
(назва навчальної дисципліни)

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

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

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

Форма навчання: денна

Рівень вищої освіти: перший (бакалаврський)

Харків 2023 рік

Розробник: _____ _____
(підпис)

Холодна Зоя Борисівна, старший викладач _____
(прізвище та ініціали, посада, науковий ступінь та вчене звання) (підпис)

Робочу програму розглянуто на засіданні кафедри комп'ютерних систем,
(назва кафедри)
мереж і кібербезпеки

Протокол № 1 від « 30 » серпня 2023 року

Завідувач кафедри д.т.н., професор _____ В'ячеслав ХАРЧЕНКО
(науковий ступінь і вчене звання) (підпис) (ім'я та прізвище)

1. Опис навчальної дисципліни

<table>
<tr><td rowspan="2">Найменування показників</td><td rowspan="2">Галузь знань,
спеціальність,
спеціалізація,
рівень вищої освіти</td><td>Характеристика навчальної дисципліни</td></tr>
<tr><td>Денна форма навчання</td></tr>
<tr><td>Кількість кредитів:
денна – 3</td><td>Галузь знань:
12 «Інформаційні технології»</td><td>Цикл професійної підготовки</td></tr>
<tr><td>Модулів – 1</td><td rowspan="4">Спеціальність:
125 «Кібербезпека»
(код і найменування)
Освітня програма:
«Безпека інформаційних і комунікаційних систем»</td><td rowspan="2">Навчальний рік
2023/2024</td></tr>
<tr><td>Змістовних модулів – 2</td></tr>
<tr><td>Індивідуальне науково-дослідне завдання: є</td><td rowspan="2">Семестр</td></tr>
<tr><td>Загальна кількість годин –
денна – 0/90</td><td>6-й</td></tr>
<tr><td rowspan="10">Тижневих годин для денної форми навчання:
аудиторних – 0
самостійної роботи студента – 90</td><td rowspan="10">Рівень вищої освіти:
перший
(бакалаврський)</td><td>Лекції</td></tr>
<tr><td>0 годин</td></tr>
<tr><td>Практичні, семнарські</td></tr>
<tr><td>0 годин</td></tr>
<tr><td>Лабораторні</td></tr>
<tr><td>0 годин</td></tr>
<tr><td>Самостійна робота</td></tr>
<tr><td>90 годин</td></tr>
<tr><td>Вид контролю</td></tr>
<tr><td>Залік</td></tr>
</table>

Співвідношення кількості годин аудиторних занять до самостійної роботи становить – *0/90.*

2. Мета та завдання навчальної дисципліни

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.

Програмні компетентності. Дисципліна має допомогти сформувати у студентів такі компетентності:

КЗ 1. Здатність застосовувати знання у практичних ситуаціях.

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

КЗ 3. Здатність професійно спілкуватися державною та іноземною мовами як усно, так і письмово.

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

КЗ 5. Здатність до пошуку, оброблення та аналізу інформації.

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

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

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

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

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

КФ 9. Здатність здійснювати професійну діяльність на основі впровадженої системи управління інформаційною та/або кібербезпеки.

КФ 11. Здатність виконувати моніторинг процесів функціонування інформаційних, інформаційно-телекомунікаційних (автоматизованих) систем згідно 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

В результаті вивчення дисципліни студенти мають досягти такі 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 5. Адаптуватися в умовах частої зміни технологій професійної діяльності, прогнозувати кінцевий результат.

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 12. Розробляти моделі загроз та порушника.

ПРН 14. Вирішувати завдання захисту програм та інформації, що обробляється в інформаційно-телекомунікаційних системах програмно-апаратними засобами та давати оцінку результативності якості прийнятих рішень.

ПРН 18. Використовувати програмні та програмно-апаратні комплекси захисту інформаційних ресурсів.

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

ПРН 20. Забезпечувати функціонування спеціального програмного забезпечення, щодо захисту інформації від руйнуючих програмних впливів, руйнуючих кодів в інформаційно-телекомунікаційних системах.

ПРН 27. Вирішувати задачі захисту потоків даних в інформаційних, інформаційно-телекомунікаційних (автоматизованих) системах.

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

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

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 53 Вирішувати задачі аналізу програмного коду на наявність можливих загроз.

Пререквізити: Дисципліна базується на знаннях, отриманих під час вивчення дисциплін уциклі загальної і професійної підготовки, передбачених навчальним планом спеціальності, а саме ОК1 «Вища математика», ОК2 «Дискретна математика», ОКЗ «Основи функціонування комп'ютерів», ОК4 «Технології програмування», ОК30 «Навчальна практика», ОК31 «Ознайомча практика»,

Кореквізити: Матеріал, засвоєний під час вивчення цієї дисципліни, є базою для дисциплін ОК33 «Кваліфікаційна робота бакалавра».

3. Зміст навчальної дисципліни

Модуль 1

Змістовний модуль 1

Тема 1. Вступ

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

Тема 2. Проектування і розроблення програмного забезпечення

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

Тема 3. Тестування програмного забезпечення

Тестування програмного продукту з використанням сучасних підходів та інструментальних засобів.

Змістовний модуль 2

Тема 4. Документування програмного забезпечення

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

Тема 5. Презентація

Створення презентацій засобами PowerPoint. Підготовка доповіді.

4. Структура навчальної дисципліни

Назви модулів і тем	Кількість годин				
	денна форма				
	усього	у тому числі			
		л	п	лаб	с.р.
1	2	3	4	5	6
Модуль 1					
Змістовний модуль 1					
1. Вступ	10				10
2. Проектування і розроблення програмного забезпечення	40				40
3. Тестування програмного забезпечення	30				30
Разом	**80**				**80**
Змістовний модуль 2					
4. Документування програмного забезпечення	5				5
5. Презентація	5				5
Разом	**10**				**10**
Усього годин	**90**				**90**

5. Теми семінарських занять

Не передбачено

6. Теми практичних занять

Не передбачено

7. Теми лабораторних занять

Не передбачено

8. Самостійна робота

№ з/п	Назва теми	Кількість годин
1	Ознайомлення з метою та програмою практики, отримання та узгодження завдання з керівником практики	5

2	Розроблення алгоритмів та їх програмна реалізація	30
3	Створення тестових наборів для перевірки розробленого програмного забезпечення	20
4	Створення звіту та оформлення його у відповідності до вимог	15
5	Створення презентації, виступ з доповіддю на звітній конференції	20
	Разом	90

9. Індивідуальні завдання

1. Відображення показників векторів магнітного поля ротора і математичний розрахунок відхилення(здвигу) магнітних полюсів шляхом апроксимації значень.
2. Покрокова демонстрація рішення задачі комівояжера жадібним методом.
3. Демонстрація роботи стека і черги.
4. Модифікована гра - Тетріс-5.
5. Порівняння двох способів знаходження посилань сайта.
6. Порівняльний аналіз алгоритмів сортування.

10. Методи навчання

Проведення консультацій, звітної конференції, а також самостійна робота здобувачівза відповідними матеріалами (п.14, 15).

11. 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.

12. Критерії оцінювання та розподіл балів, які отримують здобувачі

Складові навчальної роботи	Бали за одне заняття (завдання)	Кількість занять (завдань)	Сумарна кількість балів
Тестові набори	0...15	1	0...15
Звіт	0…40	1	0…40
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.

Критерії оцінювання роботи здобувача 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.

Шкала оцінювання: бальна і 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

13. Методичне забезпечення

Навчально-методичний комплекс дисципліни розміщений у системі управління курсами кафедри комп'ютерних систем, мереж і кібербезпеки, на сайті науково-технічної бібліотеки Національного аерокосмічного університету ім. М.Є. Жуковського «Харківський авіаційний інститут», а також у системі дистанційного навчання «Ментор».

1. Система управління курсами кафедри комп'ютерних систем, мереж і кібербезпеки [Ел. ресурс]. URL: https://elearn.csn.khai.edu
2. Навчально-методичне забезпечення дисципліни «Навчальна практика» для бакалаврів [Ел. ресурс]. URL: http://library.khai.edu/library/fulltexts/doc/ 1003Navchalna.pdf
3. Сторінка дисципліни у системі дистанційного навчання «Ментор» [Ел. ресурс]. URL: https://mentor.khai.edu

14. 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.

15. 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
3. Система управління курсами кафедри комп’ютерних систем, мереж і кібербезпеки [Ел. ресурс]. – Режим доступу: https://elearn.csn.khai.edu