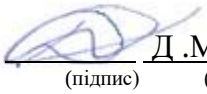
Міністерство освіти і науки України
Національний аерокосмічний університет ім. М. Є. Жуковського
«Харківський авіаційний інститут»

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

ЗАТВЕРДЖУЮ

Голова НМК



Д .М. Кри цьки й
(підпис) (ініціали та прізвище)

« 31 » сер пн я 2022 р.

РОБОЧА ПРОГРАМА ОБОВ'ЯЗКОВОЇ НАВЧАЛЬНОЇ ДИСЦИПЛІНИ

Виробнича практика
(назва навчальної дисципліни)

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

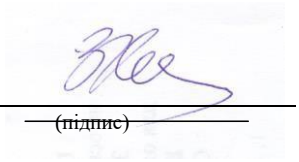
Спеціальність: 125 "Кібербезпека"
(код та найменування спеціальності)

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

Форма навчання: денна

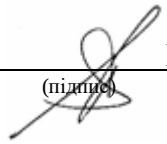
Рівень вищої освіти: перший (бакалаврський)

Харків 2022 рік

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

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

Протокол № 1 від «30» 08 2022 р.

Завідувач кафедри д .т.н., пр офесо р  В. С. Харченко
(науковий ступінь та вчене звання) (підпис) (ініціали та прізвище)

1. Опис навчальної дисципліни

<table>
<tr><td>Найменування показників</td><td>Галузь знань, спеціальність, спеціалізація, рівень вищої освіти</td><td>Характеристика навчальної дисципліни
(Денна форма навчання)</td></tr>
<tr><td>Кількість кредитів:
денна – 3</td><td rowspan="11">Галузь знань
1 2 "Інформаційні технології"
(шифр та найменування)

Спеціальність
125 "Кібербезпека"
(код та найменування)

Освітня програма
Безпека інформаційних і комунікаційних систем
(найменування)

Рівень вищої освіти:

перший (бакалаврський)</td><td>Обов’язкова</td></tr>
<tr><td>Модулів – 1</td><td rowspan="2">Навчальний рік
2022/2023</td></tr>
<tr><td>Змістовних модулів – 2</td></tr>
<tr><td>Індивідуальне науково-дослідне завдання: є</td><td>Семестр</td></tr>
<tr><td>Загальна кількість годин – денна – 0/90</td><td>6</td></tr>
<tr><td rowspan="8">Тижневих годин для денної форми навчання:
аудиторних – 0
самостійної роботи студента – 90</td><td>Лекції</td></tr>
<tr><td>0 годин</td></tr>
<tr><td>Практичні</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:

для денної форми навчання – *0/90*.

[1)] Аудиторне навантаження може бути зменшене або збільшене на одну годину в залежності від розкладу занять.

2. Мета та завдання навчальної дисципліни

Мета вивчення: використовувати знання зі створення комп'ютерних систем методами комп'ютерних наук в практиці проектування комп'ютерних систем на виробництві

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

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 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.

3. Програма 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.

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. Самостійна робота

№ з/п	Назва теми	Кількість годин
		Денна форма навчання
1	Ознайомлення з метою та програмою практики, отримання та узгодження завдання з керівником практики	10
2	Розроблення алгоритмів та їх програмна реалізація	40
3	Створення тестових наборів для перевірки розробленого програмного забезпечення	30
4	Створення звіту та оформлення його у відповідності до вимог	5
5	Створення презентації, виступ з доповіддю на звітній конференції	5
	Разом	**90**

6. Методи навчання

Проведення консультацій, звітної конференції, а також самостійна робота студентів за відповідними матеріалами (п.9, 10).

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 студенти

Структура навчальної дисципліни

8.1 Розподіл балів, які отримують студенти (кількісні критерії оцінювання)

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**

8.2 Якісні критерії оцінювання

Необхідний обсяг знань для одержання позитивної оцінки:

1. Знати принципи розроблення алгоритмів та їх програмну реалізацію.
2. Знати порядок створення тестових наборів для перевірки розробленого ПЗ.
3. Знати порядок створення звіту та оформлення його у відповідності до вимог.

Необхідний обсяг умінь для одержання позитивної оцінки:

1. Уміти розробляти алгоритми та їх програми їх реалізації.
2. Уміти створювати презентації.

8.3 Критерії оцінювання роботи

Задовільно (60-74). Показати мінімум знань та умінь. Розробити тестові набори та підготувати звіт.

Добре (75-89). Твердо знати мінімум. Розробити тестові набори та підготувати звіт з розробленням алгоритмів та презентації виконаної роботи.

Відмінно (90-100). Всі контрольні крапки здати з оцінкою "відмінно". Виступити з презентацією про виконану роботу.

Шкала оцінювання: національна та ECTS

Сума балів	Оцінка за традиційною шкалою	
	Іспит, диференційований залік	Залік
90-100	Відмінно	Зарахованно
75-89	добре	
60-74	Задовільно	
0-59	Незадовільно	Не зарахованно

9. Методичне забезпечення

Навчально-методичний комплекс дисципліни розміщений у системі управління курсами кафедри комп'ютерних систем, мереж і кібербезпеки.

1. Система управління курсами кафедри комп'ютерних систем, мереж і кібербезпеки [Ел. ресурс]. - Режим доступу: https: // elearn.csn.khai.edu.

10. 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.

Допоміжна

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

10. 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