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. Крицький
(підпис) (ініціали та прізвище)

« 31 » серпня 2022 р.

РОБОЧА ПРОГРАМА ОБОВ'ЯЗКОВОЇ НАВЧАЛЬНОЇ ДИСЦИПЛІНИ

Інформаційно-комунікаційні технології індустріальних систем
(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: Пєвнєв В. Я., доцент, д.т.н., доцент _____
(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., професор _____ В. С. Харченко
(науковий ступінь та вчене звання) (підпис) (ініціали та прізвище)

1. Опис навчальної дисципліни

<table>
<tr><td rowspan="2">Найменування показників</td><td rowspan="2">Галузь знань, напрям підготовки, рівень вищої освіти</td><td>Характеристика навчальної дисципліни</td></tr>
<tr><td>денна форма навчання</td></tr>
<tr><td>Кількість кредитів – 9</td><td rowspan="11">Галузь знань і
12 "Інформаційні технології"
(шифр та найменування)

Спеціальність 125 "Кібербезпека"
(код та найменування)

Освітня програма
Безпека інформаційних комунікаційних систем
(найменування)

Рівень вищої освіти:
перший (бакалаврський)</td><td>Обов’язкова</td></tr>
<tr><td>Кількість модулів – 2</td><td>Навчальний рік</td></tr>
<tr><td>Кількість змістових модулів – 4</td><td>2022/2023</td></tr>
<tr><td>Індивідуальне завдання: РГР</td><td rowspan="2">Семестр: 8, 7</td></tr>
<tr><td>Загальна кількість годин – 112/270</td></tr>
<tr><td rowspan="7">Кількість тижневих годин для денної форми навчання:
аудиторних – 4 самостійної роботи студента – 7</td><td>Лекції *</td></tr>
<tr><td>48 години</td></tr>
<tr><td>Практичні, семінарські*</td></tr>
<tr><td>48 години</td></tr>
<tr><td>Лабораторні*</td></tr>
<tr><td>0 годин</td></tr>
<tr><td>Самостійна робота</td></tr>
<tr><td>158 годин</td><td>Індивідуальні завдання</td></tr>
<tr><td>16 годин</td><td>Вид контролю</td></tr>
<tr><td>іспит</td></tr>
</table>

Співвідношення кількості годин аудиторних занять до самостійної роботи становить: Для денної форми навчання – 112/158.

* Аудиторне навантаження може бути зменшене або збільшене на одну годину в залежності від розкладу занять.

2. Мета та завдання навчальної дисципліни

Мета вивчення: вивчення можливостей та технологій сучасних інформаційно-комунікаційні мереж (ІКМ), основ їх побудови, супроводу і адміністрування.

Завдання: вивчення основних принципів побудови ІКМ; вивчення локальних ІКМ; вивчення мережевих архітектурних рішень; вивчення протоколів нижнього рівня ІКМ; вивчення питань проектування ІКМ; вивчення протоколів середнього і верхнього рівня ІКМ; вивчення способів адміністрування ІКМ.

Компетентності, які набуваються:

– здатність застосовувати знання у практичних ситуаціях;
– здатність та розуміння предметної області та розуміння професії;
– здатність професійно спілкуватися державною та іноземною мовами як усно, так і письмово;
– вміння виявити, ставити та вирішувати проблеми за професійним спрямуванням;
– здатність до пошуку, оброблення та аналізу інформації;
– здатність до використання інформаційно-комунікаційних технологій сучасних методів і моделей інформаційної безпеки та/або кібербезпеки;
– здатність до використання програмно та програмно-апаратних комплексів засобів захисту інформації в інформаційно-телекомунікаційних
– (автоматизованих) системах.

Очікувані результати навчання:

– застосовувати знання державної та іноземних мов з метою забезпечення ефективності професійної комунікації;
– організовувати власну професійну діяльність, обирати оптимальні методи та способи розв’язування складних спеціалізованих задач та практичних проблем у професійній діяльності, оцінювати їхню ефективність;
– використовувати результати самостійного пошуку, аналізу та синтезу інформації з різних джерел для ефективного рішення спеціалізованих задач професійної діяльності;
– 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;
– готувати пропозиції до нормативних актів щодо забезпечення інформаційної та /або кібербезпеки
– виконувати аналіз та декомпозицію інформаційно-телекомунікаційних систем.

– виконувати аналіз зв’язків між інформаційними процесами на віддалених обчислювальних системах.

– аналізувати проекти інформаційно-телекомунікаційних систем базуючись на стандартизованих технологіях та протоколах передачі даних.

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

– використовувати сучасне програмно-апаратне забезпечення інформаційно-комунікаційних технологій.

– забезпечувати процеси захисту та функціонування інформаційно-телекомунікаційних (автоматизованих) систем на основі практик, навичок та знань, щодо структурних (структурно-логічних) схем, топології мережі, сучасних архітектур та моделей захисту електронних інформаційних ресурсів з відображенням взаємозв’язків та інформаційних потоків, процесів для внутрішніх і віддалених компонент.

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

– реалізовувати заходи з протидії отриманню несанкціонованого доступу до інформаційних ресурсів і процесів в інформаційних та інформаційно-телекомунікаційних (автоматизованих) системах.

– вирішувати задачі управління доступом до інформаційних ресурсів та процесів в інформаційних та інформаційно-телекомунікаційних (автоматизованих) системах на основі моделей управління доступом (мандатних, дискреційних, рольових).

– впроваджувати заходи та забезпечувати реалізацію процесів попередження отриманню несанкціонованого доступу і захисту інформаційних, інформаційно-телекомунікаційних (автоматизованих) систем на основі еталонної моделі взаємодії відкритих систем.

– вирішувати задачі захисту потоків даних в інформаційних, інформаційно-телекомунікаційних (автоматизованих) системах.

– застосовувати теорії та методи захисту для забезпечення безпеки елементів інформаційно-телекомунікаційних систем.

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

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

– вирішувати задачі захисту інформації, що обробляється в інформаційно-телекомунікаційних системах з використанням сучасних методів та засобів криптографічного захисту інформації.

Пререквізити – дисципліна базується на «Системи технічного захисту інформації», «Інформаційно-комунікаційні системи».

Кореквізити – «Дипломний робота (проект) бакалавра».

3. Програма навчальної дисципліни

Модуль 1. Основи аналізу безпеки

Змістовний модуль 1. Базові поняття безпеки.

Тема 1. Предмет, мета вивчення і задачі дисципліни.

Предмет, мета вивчення і задачі дисципліни. Структура і зміст дисципліни, а також методичні рекомендації по її вивченню. Місце дисципліни в навчальному процесі. Вимоги до знань і умінь студентів. Характеристика рекомендованих під час вивчення дисципліни джерел інформації.

Тема 2. Загальні відомості про безпеку індустріальних систем.

Тенденції розвитку індустріальних систем у контексті глобальної ініціативи «Індустрія 4.0».

Архітектура існуючих індустріальних систем: «Інтернет речей», автоматизовані системи управління технологічними процесами (АСУ ТП), вбудовані системи, програмовані логічні контролери (ПЛК).

Головні риси, які відрізняють сучасні індустріальні системи («Індустрія 4.0») від систем попередніх поколінь. Приклади програмно-технічних рішень.

Задачі забезпечення інформаційної та функціональної безпеки при зрощенні технологій «Інтернет речей» та АСУ ТП. Ризики експлуатації індустріальних систем. Джерела ризиків та приклади порушень безпеки.

Властивості індустріальних систем. Головні атрибути інформаційної та функціональної безпеки. Структура вимог до інформаційної та функціональної безпеки.

Структура вивчення навчальної дисципліни “Теорія і методи безпеки індустріальних систем”. Структура Assurance Case, як збірника артефактів оцінювання та забезпечення безпеки.

Тема 3. Вимоги стандартів щодо безпеки індустріальних систем.

Огляд стандартів з інформаційної та функціональної безпеки індустріальних систем.

Стандарт МЕК 61508 «Функціональна безпека систем електричних, електронних, програмованих електронних, пов'язаних з безпекою». Зв'язки між частинами МЕК 61508 та короткий зміст частин.

Систематизація вимог до інформаційної та функціональної безпеки. Приклади успішної сертифікації контролерів щодо вимог МЕК 61508.

Змістовний модуль 2. Керування та оцінювання безпеки.

Тема 1. Менеджмент інформаційної та функціональної безпеки.

Порівняння менеджменту інформаційної та функціональної безпеки. План керування функціональною безпекою та його зв'язок з системою менеджменту інформаційної безпеки.

План керування персоналом. План керування конфігурацією. Керування зміненнями. Вибір та оцінювання програмних засобів розробки. План верифікації та валідації. План документування та структура документів з безпеки.

Оцінювання та аудит інформаційної та функціональної безпеки.

Тема 2. Життєвий цикл інформаційної та функціональної безпеки.

Поняття життєвого циклу. Повний життєвий цикл та життєвий цикл розробки. V-образний життєвий цикл.

Етап «Концепція». Етап «Вимоги». Етап «Архітектурний проект». Етап «Проект програмного забезпечення». Етап « Проект технічних засобів». Етап «Кодування програмного забезпечення».

Етап «Тестування програмного забезпечення». Етап «Інтеграційне тестування». Етап «Валідація». Етап «Введення до експлуатацій». Етап «Експлуатація та супроводження». Етап «Зняття з експлуатації».

Планування життєвого циклу.

Тема 3. Оцінювання функціональної безпеки.

Структура атрибутів інформаційної та функціональної безпеки. Підхід до аналізу ризиків індустріальних систем та встановлення рівнів інтегрованості функціональної безпеки.

Зв'язок показників надійності та функціональної безпеки. Інтенсивності безпечних та небезпечних, діагностовних та недіагностовних відмов. Середня імовірність небезпечної відмови за запитом функції безпеки. Середня частота небезпечних відмов функції безпеки. Доля безпечних відмов. Діагностичне покриття.

Вимоги до кількісних показників функціональної безпеки ІУС згідно IEC 61508. Методологія аналізу видів, режимів та критичності відмов (FMECA). Оптимізація структури ІУС за показниками готовності та критерієм функціональної безпеки.

Модуль 2. Основи забезпечення безпеки

Змістовний модуль 1. Огляд підходів до забезпечення безпеки індустріальних систем.

Тема 1. Методи забезпечення функціональної безпеки індустріальних систем.

Топологічні та конструктивні особливості індустріальних систем. Типові програмно-апаратні рішення із забезпечення функціональної безпеки індустріальних систем.

Багатоканальні архітектури. Резервування комп’ютерної мережі. Резервування електроживлення. Захист від падіння та підвищення напруги електроживлення. Принцип незалежності та фізичне і логічне розділення компонентів.

Самодіагностування. Контроль конфігурації апаратно-програмних засобів. Контроль часових параметрів функціонування програмного забезпечення. Сторожовий таймер. Контроль точності та діагностування аналогових входів та

виходів. Автоматичний перехід вихідних сигналів у безпечній стан. Контроль комунікацій та циклічні коди (CRC).

Захист від зовнішніх впливів: вентиляція та контроль температури, екранування та фізичне розподілення кабелів, вібростійкість, корозостійкість, захист від вологи та пилу.

Використання якісних компонентів. Принцип діверсності.

Типові організаційні заходи із забезпечення функціональної безпеки індустріальних систем. Управління проектами.

Формальні та полуформальні нотації для розробки специфікації вимог та проектів індустріальних систем та програмних і апаратних компонентів. Структурований процес розробки системи та програмного забезпечення. Використання кращих практик та стандартів безпечного програмування.

Використання сертифікованих компіляторів та трансляторів коду та сертифікованих бібліотек програмних компонентів.

Виконання всебічних оглядів, аналізу та тестування при верифікації та валідації. Контроль якості при виробництві апаратних компонентів.

Ергономічний людино-машинний інтерфейс та захист від помилок оператора. Підтримка захисту від несанкціонованого доступу. Супроводження при експлуатації та врахування опиту експлуатації.

Тема 2. Особливості забезпечення інформаційної безпеки індустріальних систем.

Огляд стандартів з інформаційної безпеки індустріальних систем. Порівняльний аналіз властивостей індустріальних та інформаційних систем.

Структура гармонізованих вимог до інформаційної та функціональної безпеки індустріальних систем.

Оцінювання ризиків та управління ризиками. Організація управління безпекою за тріадою «Персонал – Процеси – Технології».

Контекст вимог до індустріальних систем та моделі індустріальних систем. Концепція рівнів інформаційної безпеки та зонування обладнання індустріальних систем.

Змістовний модуль 2. Застосування методології Assurance Case з врахуванням вимог до функціональної та інформаційної безпеки.

Тема 1. Управління вимогами до безпеки.

Процес інженерії вимог. Ідентифікація та аналіз вимог. Верифікація і валідація вимог. Забезпечення якості вимог. Пряме та зворотне трасування вимог. Програмні засоби підтримки трасування вимог.

Тема 2. Методи тестування індустріальних систем.

Організація процесу верифікації та вилідації індустріальних систем та її програмно-апаратних компонентів.

Огляд специфікації вимог. Огляд специфікації архітектурного проекту. Огляд проекту апаратних засобів.

Аналіз надійності та аналіз видів, режимів та критичності відмов (FMECA).

Огляд проекту програмного забезпечення. Огляд та статичний аналіз програмного коду. Тестування програмного коду.

Особливості верифікації та валідації індустріальних систем на базі програмованих логічних інтегральних схем (ПЛІС).

Тестування із засівом дефектів. Інтеграційне тестування. Валідаційне тестування. Тестування на стійкість до зовнішніх впливів.

Тема 3. Методологія Assurance Case.

Зміст та теоретичні основи методології Assurance Case. Формальна нотація CAE (Claim – Argument – Evidence). Формальна нотація GSN (Goal Structured Notation). Інтеграція методології Assurance Case у життєвий цикл індустріальних систем. Програмні засоби підтримки методології Assurance Case.

4. Структура навчальної дисципліни

Назви змістових модулів і тем	Кількість годин				
	Денна форма				
	Усього	У тому числі			
		л	п	лаб	с.р.
1	2	3	4	5	7
Модуль 1					
Змістовий модуль 1. Базові поняття безпеки.					
Тема 1. Предмет, мета вивчення і задачі дисципліни.	1	1			
Тема 2. Загальні відомості про безпеку індустріальних систем.	12	3			9
Тема 3. Вимоги стандартів щодо безпеки індустріальних систем.	13	2		2	9
Разом за змістовим модулем 1	26	6		2	18
Змістовий модуль 2. Керування та оцінювання безпеки.					
Тема 1. Менеджмент інформаційної та функціональної безпеки	15	2		4	9
Тема 2. Життєвий цикл інформаційної та функціональної безпеки.	13	4			9
Тема 3. Оцінювання функціональної безпеки.	17	4		4	9
Разом за змістовим модулем 2	45	10		8	27
Усього годин	**71**	**16**		**10**	**45**
Модуль 2					
Змістовий модуль 1. Огляд підходів до забезпечення безпеки індустріальних систем.					
Тема 1. Методи забезпечення функціональної безпеки індустріальних систем.	17	4		4	9
Тема 2. Особливості забезпечення інформаційної безпеки індустріальних систем.	15	2		4	9
Разом за змістовим модулем 1	32	6		8	18
Змістовий модуль 2. Застосування методології Assurance Case з врахуванням вимог до функціональної та інформаційної безпеки.					
Тема 1. Управління вимогами до безпеки.	15	2		4	9
Тема 2. Методи тестування індустріальних систем..	17	4		4	9
Тема 3. Методологія Assurance Case.	15	2		4	9
Разом за змістовим модулем 2	47	8		12	27
Усього годин	**79**	**14**		**20**	**45**

5. Теми семінарських занять

№ з/п	Назва теми	Кількість Годин
1	*Не передбачено*	
	Разом	

6. Теми практичних занять

№ з/п	Назва теми	Кількість Годин
1	*Не передбачено*	
	Разом	

7. Теми лабораторних занять

№ з/п	Назва теми	Кількість годин
1	Аналіз вимог стандартів у галузі безпеки індустріальних систем	2
2	Складання плану керування функціональною безпекою	4
3	Розрахунок показників безпеки за допомогою програмного засобу SISTEMA (http://www.dguv.de/ifa/praxishilfen/practical-solutions-machine-safety/software-sistema/index.jsp)	4
4	Розробка специфікації вимог та системи управління на базі програмно-апаратної платформи Arduino з використанням типових рішень із забезпечення функціональної безпеки	4
5	Аналіз та вибір засобів забезпечення інформаційної безпеки індустріальних систем	4
6	Трасування вимог до безпеки індустріальних систем	4
7	Розробка тестової документації та тестування системи управління на базі програмно-апаратної платформи Arduino	4
8	Використання програмних засобів підтримки методології Assurance Case	4
	Разом	**30**

8. Самостійна робота

№ з/п	Назва теми	Кількість годин
1	Властивості сучасних індустріальних систем за версією National Institute of Standards and Technologies (на прикладі документу NIST SP 800-82, Guide to Industrial Control Systems Security)	9
2	Зміст стандартів серії МЕК 61508	9
3	Звід знань щодо менеджменту проектів (PMBOK) у частині керування персоналом та керування конфігураціями	9
4	Життєвий цикл критичного програмного забезпечення (згідно МЕК 61508-3)	9
5	Розрахунок показників надійності систем безпеки (згідно ABB Safety Handbook)	9
6	Методи за заходи захисту від випадкових та систематичних відмов (згідно МЕК 61508-7)	9
7	Глосарій термінів та сіллабус щодо підготовки професіоналів з інженерії вимог	9
8	Глосарій термінов та сілабус щодо підготовки професіоналів з тестування	9
9	Зміст стандартів серії МЕК 62443	9
10	Стандарт з нотації GSN (Structured Goal Notation)	9
	Разом	**90**

9. Індивідуальні завдання

Не передбачено

10. Методи навчання

Проведення аудиторних лекцій, практичних, лабораторних занять, консультацій, а також самостійна робота студентів за матеріалами, опублікованими кафедрою.

11. Методи контролю

Проведення поточного контролю, тестування знань, підсумковий контроль у вигляді екзамену.

12. Розподіл балів, які отримують студенти

Поточне тестування і самостійна робота	Сума	Підсумковий тест (залік/іспит) у разі відмови від балів поточного тестування та за наявності допуску до заліку/іспиту

Модуль 1	Модуль 2		
Т1-Т3, Т1-Т3	Т1-Т3, Т1-Т2		
50	50	100	100

Т1 ... Т10 – теми змістовних модулів.

Шкала оцінювання: національна та ECTS

Сума балів за всі види навчальної діяльності	Оцінка ECTS	Оцінка за національною шкалою	
		для екзамену, курсового проекту (роботи), практики	для заліку
90-100	**A**	відмінно	зараховано
83-89	**B**	добре	
75-82	**C**		
68-74	**D**	задовільно	
60-67	**E**		
01-59	**FX**	незадовільно з можливістю повторного складання	не зараховано з можливістю повторного складання

13. Методичне забезпечення

1. Скляр В.В. Конспект лекцій.
2. Скляр В.В. Методичні рекомендації для виконання лабораторних робот.

14. Рекомендована література

Базова

1. 1. Федоров, Ю.М. Довідник інженера з АСУ ТП: Проектування та розробка [Текст]/Ю.М. Федоров. - М.: Інфра-Інженерія, 2008. - 928 с.
2. Leveson, N. Engineering a Safer World: Systems Thinking Applied to Safety [Text] / N. Leveson. – The MIT Press, 2011. – 534 p.
3. Smith, D. Functional Safety. A Straightforward Guide to applying IEC 61508 and Related Standards [Text] / D. Smith, K. Simpson. – Elsevier Butterworth-Heinemann, Oxford, UK, 2004. – 263 p.
4. Medoff, M. Functional Safety – An IEC 61508 SIL 3 Compatible Development Process [Text] / M. Medoff, R. Faller. – exida.com L.L.C., Sellersville, PA, USA, 2010. – 281 p.
5. Basilio, A. Functional Safety of Safety–Related Systems. Manual for Plant Engineering and Maintenance [Text] / A. Basilio, F. Landrini, G. Novelli, G. Landrini, M. Baldrigh]. – G.M. International S.r.l, Villasanta, Italy, 2008. – 388 p

6.Тюрін, О.Г. Управління потенційно небезпечними технологіями [Текст]/О.Г. Тюрін, В.С. Кальницький, Є.Ф. Жегрів. - М.: Інфра-Інженерія, 2011, 288 с.
7.Скляр, В.В. Забезпечення безпеки АСУТП відповідно до сучасних стандартів [Текст] / В.В. Скляр. - М.: Інфра-Інженерія, 2018, 384 с.

Допоміжна

8. NIST SP 800-82 Revision 2, Guide to Industrial Control Systems (ICS) Security: Supervisory Control and Data Acquisition (SCADA) Systems, Distributed Control Systems (DCS), and Other Control System Configurations such as Programmable Logic Controllers (PLC). – National Institute of Standards and Technologies, 2015.
9. Посібник зі зведення знань з управління проектами (Підручник PMBOK®), П'яте видання. - Project Management Institute, Inc., 2013.ГОСТ Р МЭК 61508, Функциональная безопасность систем электрических, электронных, программируемых электронных, связанных с безопасностью [Электронный ресурс]. – Режим доступа: http://standartgost.ru/.
10. ABB Safety Handbook. Machine Safety – Jokab Safety products. – ABB, 2013.
11. Syllabus: REQB® Certified Professional for Requirements Engineering. Foundation Level, Version 2.1. – Requirements Engineering Qualification Board, 2014.
12. Standard glossary of terms used in Requirements Engineering, Version 1.3. – Requirements Engineering Qualification Board, 2014.
13. Certified Tester Foundation Level Syllabus. – International Software Testing Qualifications Board, 2011.
14. Standard glossary of terms used in Software Testing, Version 2.3. – International Software Testing Qualifications Board, 2014.
15. GSN Community Standard ,Version 1. – Origin Consulting (York) Limited, 2011.

15. Інформаційні ресурси

1.Вікіпедія – свобідна енциклопедія [Електрон. ресурс]. – Режим доступу: http://www. ru.wikipedia.org/.
2.Публікації з кібербезпеки National Institute of Standards and Technologies [Електрон. ресурс] – Режим доступу: http://csrc.nist.gov/publications/PubsSPs.html#SP 800/.
3.Електронний ресурс інженерів з інформаційних технологій «Хабрахабр» (хаб «Промислове програмування») [Електрон. ресурс] – Режим доступу: https://habrahabr.ru/hub/industrial_control_system/.
4.Асоціація підприємств промислової автоматизації України (АППАУ) [Електрон. ресурс] – Режим доступу: http://appau.org.ua/.