

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

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

ЗАТВЕРДЖУЮ

Гарант освітньої програми



(підпис)

Д.Д.Узун

(ініціали та прізвище)

« 31 » серпня 2021 р

**РОБОЧА ПРОГРАМА
ВИБІРКОВОЇ НАВЧАЛЬНОЇ ДИСЦИПЛІНИ**

Стандартизація і сертифікація систем кібербезпеки
(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 (1 рік 4 місяці)
(найменування освітньої програми)

Форма навчання: денна

Рівень вищої освіти: другий (магістерський)

Харків 2021 рік

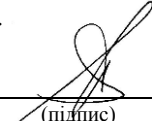
Розробник: Ілляшенко О.О., доцент, к.т.н.
(прізвище та ініціали, посада, науковий ступінь та вчене звання)


(підпис)

Робочу програму розглянуто на засіданні кафедри _____
«Комп'ютерних систем, мереж і кібербезпеки»
(назва кафедри)

Протокол № 1 від « 30 » 08 2021 р.

Завідувач кафедри д.т.н., професор
(науковий ступінь та вчене звання)


(підпис)

В. С. Харченко
(ініціали та прізвище)

1. Опис навчальної дисципліни

Найменування показників	Галузь знань, спеціальність, освітня програма, рівень вищої освіти	Характеристика навчальної дисципліни (денна форма навчання)
Кількість кредитів – 4	<p style="text-align: center;">Галузь знань <u>12 "Інформаційні технології"</u> (шифр та найменування)</p> <p style="text-align: center;">Спеціальність <u>125 "Кібербезпека"</u> (код та найменування)</p> <p style="text-align: center;">Освітня програма <u>Безпека інформаційних і комунікаційних систем</u> <u>Кібербезпека</u> <u>індустріальних систем</u> (найменування)</p> <p style="text-align: center;">Рівень вищої освіти: другий (магістерський)</p>	Вибіркова
Кількість модулів – 2		Навчальний рік
Кількість змістових модулів – 4		2021/ 2022
Індивідуальне завдання: <u>немає</u>		Семестр
Загальна кількість годин – 48 / 120		<u>2-й</u>
Кількість тижневих годин для денної форми навчання: аудиторних – 2/1 самостійної роботи студента – 4/4		Лекції
		<u>32</u> годин
		Практичні, семінарські
		<u>16</u> годин
		Лабораторні
	<u>0</u> годин	
	Самостійна робота	
<u>72</u> годин		
Вид контролю		
іспит		

Співвідношення кількості годин аудиторних занять до загальної кількості годин становить: 48/120.

2. Мета та завдання навчальної дисципліни

Мета вивчення: оволодіння студентами знаннями щодо методів та засобів розробки енергоефективних систем та програм-но-апаратних комплексів.

Завдання: (ВБ1.4) формування у студентів фахових знань щодо існуючих методів оцінювання енергоефективності проектних рішень, набуття практичних навичок у сфері розробки та впровадження новітніх технологій забезпечення енергоефективності програмно-апаратних комплексів вбудованих систем.

Компетентності, які набуваються: Дисципліна має допомогти сформувати у студентів такі компетентності:

- здатність до абстрактного мислення, аналізу та синтезу
- здатність планувати та управляти часом
- навички використання інформаційних і комунікаційних технологій
- здатність до пошуку, оброблення та аналізу інформації з різних джерел
- здатність бути критичним і самокритичним
- здатність генерувати нові ідеї (креативність)
- здатність приймати обґрунтовані рішення
- здатність розробляти та управляти проектами
- прихильність безпеці
- здатність оцінювати та забезпечувати якість виконуваних робіт.
- визначеність і наполегливість щодо поставлених завдань і взятих обов'язків
- базові знання фундаментальних наук в обсязі, необхідному для освоєння загально професійних дисциплін
- вміння виявляти, аналізувати та вирішувати проблеми у професійній сфері
- здатність використовувати вимоги національних та міжнародних стандартів та нормативно-правової бази у сфері забезпечення кібербезпеки під час виконання професійних задач з проектування, розробки, впровадження та застосування системи та методів забезпечення кібербезпеки та захисту інформації

Очікувані результати навчання: В результаті вивчення дисципліни студенти мають досягти такі програмні результати навчання:

- уміти грамотно висловлюватися в усній та писемній формі
- здатність використовувати мову професійного спілкування
- вміти аргументувати свої думки
- вміти аналізувати матеріал і робити висновки
- пошук інформації в різних джерелах для розв'язання задач спеціальності
- здатність продемонструвати розуміння впливу рішень у суспільному і соціальному контексті
- розуміти й інтерпретувати вивчене
- використовувати вивчений матеріал у нових ситуаціях

Пререквізити: Матеріал дисципліни базується на знаннях, отриманих під час вивчення дисципліни із циклу професійної підготовки, а саме "Математичні методи моделювання та оптимізації процесів".

Кореквізити: Необхідними супутніми дисциплінами є дисципліни з циклу вибіркових дисциплін, а саме «Методи та технології кібербезпеки критичних інфраструктур», «Моніторинг, аудит та економіка безпечних ІКС».

3. Програма навчальної дисципліни

Модуль 1. Стандартизація методів та засобів захисту інформації

Змістовний модуль 1. Науково-методичні основи стандартизації

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. Суть стандартизації та організація стандартизації в Україні.

Головні принципи стандартизації. Етапи стандартизації. Суть стандартизації та організація стандартизації в галузі захисту інформації в Україні.

Особливості стандартизації засобів захисту інформації. Організаційна система стандартизації.

Змістовний модуль 2. Методологічні основи забезпечення інформаційної безпеки.

Тема 1. Міжнародні стандарти з основ забезпечення безпеки інформації та кібербезпеки

Нормативні документи із методологічних основ забезпечення інформаційної безпеки. Міжнародні стандарти ISO/IEC 17799 та ISO/IEC 13355. Загальна модель забезпечення інформаційної безпеки в корпоративних системах. Політика безпеки. Домени та політика безпеки. Послуги та механізми безпеки. Управління безпекою. Менеджмент безпеки. Вимоги міжнародного стандарту ISO/IEC 17799 та стандарту BSI. Інжиніринг систем безпеки. Управління ризиками. Базова модель безпеки інформаційних технологій. Основні положення безпеки інформації. Стандарт ISO/IEC 10181. Архітектура безпеки ВОС, вимоги стандарту ISO/IEC 7498. Базова технічна модель безпеки ІТ-систем. Критерії оцінки безпеки інформаційних технологій. Вимоги міжнародного стандарту ISO/IEC 15408. Функціональний підхід до оцінки безпеки. Вимоги національного стандарту НД ТЗІ 2.5-004-1999.

Тема 2. Стандартизація механізмів кібербезпеки.

Стандарти механізмів конфіденціальності. Основні міжнародні стандарти механізмів безпеки. Реєстр алгоритмів (ISO/IEC 9979). Режими роботи алгоритмів блочного шифрування: практичні рекомендації стандарту ISO/IEC

10116. Вимоги до блочних та поточних систем шифрування (стандарт ISO/IEC 18033). Методи формування кодів автентифікації повідомлень. Стандарт ISO/IEC 9797. Призначення стандарту ISO/IEC 9797. Формування MAC-кодів на базі алгоритмів блочного шифрування. Формування MAC-кодів з використанням хеш-функцій. Методи формування цифрових підписів. Стандарти ISO/IEC 9796 та ISO/IEC 14888. Призначення стандартів. Основні визначення. Цифровий підпис з відновленням повідомлення. Цифровий підпис з додаванням. Методи формування хеш-кодів, механізм невідмовності. Стандарти ISO/IEC 10118 та ISO/IEC 13888. Алгоритми хешування на базі блочних шифрів. Призначені хеш-функції SHA-1, RIPEMD-128, RIPEMD-160. Хеш-функції на базі модулярної арифметики. Механізм невідмовності.

Тема 3. Методи управління ключами.

Основні положення управління ключами. Стандарт ISO/IEC 11770. Призначення стандарту. Основні визначення. Механізми управління ключами методами симетричної криптографії. Механізми управління ключами методами несиметричної криптографії. Сертифікація ключів. Треті довірчі сторони

Модуль 2. СЕРТИФІКАЦІЯ ЗАСОБІВ ЗАХИСТУ ІНФОРМАЦІЇ.

Змістовний модуль 1. Науково-методологічні та організаційні основи сертифікації та ліцензування діяльності в галузі захисту інформації та кібербезпеки

Тема 1. Основи сертифікації та ліцензування діяльності в галузі захисту інформації.

Загальні положення та принципи сертифікації. Огляд вітчизняних стандартів з сертифікації. Основні положення системи сертифікації. Органи сертифікації. Вимоги до органів сертифікації, випробувальних центрів та лабораторій. Національна система ліцензування діяльності в галузі захисту інформації. Нормативно-правова база ліцензування. Ліцензійні вимоги та порядок їх перевірки. Система сертифікації засобів КЗІ та порядок проведення сертифікаційних іспитів та експертиз (тематичних досліджень)ї. Нормативна база сертифікації та експертизи засобів КЗІ. Система сертифікації засобів КЗІ. Порядок проведення сертифікації та експертизи. Практичні рекомендації стандартів.

Тема 2. Основи аудиту інформаційної та кібербезпеки

Загальні положення аудиту безпеки. Порядок проведення аудиту. Етичні норми аудитора. Методики проведення аудиту за міжнародними та регіональними стандартами інформаційної безпеки.

4. Структура навчальної дисципліни

Назви змістових модулів і тем	Кількість годин				
	Усього	Денна форма			
		У тому числі			
		л	п	лаб.	с. р.
1	2	3	4	5	6
Модуль 1					
Змістовий модуль 1. Науково-методичні основи стандартизації					
Тема 1. Предмет, мета вивчення і задачі дисципліни	8	2			6
Тема 2. Суть стандартизації та організація стандартизації в Україні	12	4	2		6
Разом за змістовним модулем 1	20	6	2		12
Змістовний модуль 2. Методологічні основи забезпечення інформаційної безпеки					
Тема 1. Міжнародні стандарти з основ забезпечення безпеки інформації та кібербезпеки	17	5	2		10
Тема 2. Стандартизація механізмів кібербезпеки	22	8	4		10
Тема 3. Методи управління ключами	15	5			10
Разом за змістовним модулем 2	54	18	6		30
Разом за модулем 1	74	24	8		42
Модуль 2					
Змістовний модуль 1. Науково-методологічні та організаційні основи сертифікації та ліцензування діяльності в галузі захисту інформації та кібербезпеки					
Тема 1. Основи сертифікації та ліцензування діяльності в галузі захисту інформації	20	4	4		15
Тема 2. Основи аудиту інформаційної та кібербезпеки	23	4	4		15
Разом за змістовним модулем 1	46	8	8		30
Усього годин	120	32	16		72

5. Теми семінарських занять

№ з/п	Назва теми	Кількість годин	
		Денна форма навчання	
1	<i>Не передбачено</i>		
	Разом		

6. Теми практичних занять

№ з/п	Назва теми	Кількість годин
		Денна форма навчання
1	Розроблення елементів профілю захисту у відповідності до вимог міжнародного стандарту ISO/IEC 15408	6
2	Статистичні дослідження властивостей генераторів випадкових та псевдовипадкових послідовностей	5
3	Оцінка рівня зрілості процесів захисту інформації в організації	5
	Разом	16

7. Теми лабораторних занять

№ з/п	Назва теми	Кількість годин
		Денна форма навчання
1		
	Разом	

8. Самостійна робота

№ з/п	Назва теми	Кількість годин
		Денна форма навчання
1	Предмет, мета вивчення і задачі дисципліни.	10
2	Суть стандартизації та організація стандартизації в Україні.	10
3	Міжнародні стандарти з основ забезпечення безпеки інформації та кібербезпеки.	20
4	Стандартизація механізмів кібербезпеки	20
5	Методи управління ключами	14
6	Основи сертифікації та ліцензування діяльності в галузі захисту	23
7	Основи аудиту інформаційної та кібербезпеки	20
	Разом	117

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. Критерії оцінювання та розподіл балів, які отримують здобувачі

Складові навчальної роботи	Бали за одне заняття (завдання)	Кількість занять (завдань)	Сумарна кількість балів
Змістовний модуль 1			
Практичні заняття	0...10	4	0...40
Змістовний модуль 2			
Практичні заняття	0...10	4	0...40
Підсумковий контроль	0...20	3	0...20
Усього за семестр			0...100

Критерії оцінювання роботи здобувача протягом семестру

1. *Задовільно* (60-74). Показати мінімум знань та умінь. Захистити не менше 80% від усіх завдань практичних занять. Знати основні міжнародні та національні нормативні документи зі стандартизації та сертифікації інформаційних систем.

2. *Добре* (75-89). Твердо знати необхідний обсяг знань для одержання позитивної оцінки, захистити не менше 90% завдань практичних занять. Уміти використовувати практичні навички з використання міжнародних та національних нормативних документів зі стандартизації та сертифікації інформаційних систем для розроблення елементів профілю захисту у відповідності до вимог міжнародного стандарту ISO/IEC 15408.

Відмінно (90-100). Здати всі контрольні точки з оцінкою «відмінно». Досконально знати всі теми та уміти їх застосовувати. Уміти застосовувати навички для розроблення елементів профілю захисту у відповідності до вимог міжнародного стандарту ISO/IEC 15408, для проведення статистичних досліджень властивостей генераторів випадкових та псевдовипадкових послідовностей, вміти проводити оцінювання рівня зрілості процесів захисту інформації в організації.

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.

1. Потій О. В. Конспект лекцій.
2. Потій О. В. Лабораторні роботи.
3. Потій О. В. Методичні вказівки щодо виконання лабораторних робіт.

14. Рекомендована література

Базова

1. Шаповал М.І. Основи стандартизації, управління якістю і сертифікації. – К.:2000. – 174 с.
2. Горбенко Ю.І. Побудування та аналіз систем, протоколів і засобів криптографічного захисту інформації. Ч. !. Методи побудування та аналізу, стандартизації та застосування криптографічних систем / Харків: Форт, 2015. – 960 с.
3. Сертифікація в Україні. Нормативні акти та інші документи. Т. 1,2,3. Київ, 1998.
4. Потій О.В. Конспект лекцій з дисципліни “Стандартизація та сертифікація в галузі захисту інформації”. Стандарти механізмів безпеки. – Харків, ХНУРЕ, 2001 – 80 с.
5. Потій О.В. Конспект лекцій з дисципліни “Стандартизація та сертифікація в галузі захисту інформації”. Стандарти управління ключами – Харків, ХНУРЕ, 2002 – 80 с.

Допоміжна

1. Радіотехніка. Всеукраїнська міжвідомча науково-технічний збірник. Тематичний випуск «Інформаційна безпека». Випуски – 2015-2018.
2. Правове, нормативне та метрологічне забезпечення системи захисту інформації в Україні. Науково технічний збірник. – 2015- 2018.

15. Інформаційні ресурси

1. Міжнародні стандарти Режим доступу: <https://www.iso.org/ru/home.html>
2. Європейські стандарти. Режим доступу: <https://www.etsi.org/standards#Security>
3. Національні нормативні документи: <https://cip.gov.ua/ua/docs>