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

Керівник проектної групи

_____ А.В. Горбенко
(підпис) (ініціали та прізвище)

« 30 » серпня 2019 р.

РОБОЧА ПРОГРАМА ВИБІРКОВОЇ НАВЧАЛЬНОЇ ДИСЦИПЛІНИ

Стандартизація та 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»
(найменування освітньої програми)

Форма навчання: денна

Рівень вищої освіти: другий (магістерський)

Харків 2019 рік

Робоча програма «Стандартизація та сертифікація систем кібербезпеки»
(назва дисципліни)

для студентів за спеціальністю 125 «Кібербезпека» освітньої програми
(код та найменування спеціальності)

«Безпека інформаційних і комунікаційних систем»
(назви освітньої програми)

« 26 » серпня 2019 р. , – 9 с.

Розробник: Потій Олександр Володимирович, професор, д.т.н., професор
(прізвище та ініціали, посада, науковий ступінь та вчене звання)

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

Протокол № 1 від « 30 » серпня 2019 року

Завідувач кафедри комп'ютерних систем, мереж і кібербезпеки
(назва 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, спеціальність, спеціалізація, рівень вищої освіти</td><td>Характеристика навчальної дисципліни</td></tr>
<tr><td>Денна форма навчання</td></tr>
<tr><td>Кількість кредитів: 4</td><td>Галузь знань:
12 «Інформаційні технології»</td><td>Цикл професійної підготовки</td></tr>
<tr><td>Модулів – 2</td><td rowspan="4">Спеціальність:
125 «Кібербезпека»

Освітня програма:
«Безпека інформаційних і комунікаційних систем»
«Безпека індустріальних систем»</td><td rowspan="2">Навчальний рік
2019/2020</td></tr>
<tr><td>Змістових модулів – 4</td></tr>
<tr><td>Індивідуальне науково-дослідне завдання: немає</td><td rowspan="2">Семестр</td></tr>
<tr><td>Загальна кількість годин – денна – 48/72</td><td>10</td></tr>
<tr><td rowspan="11">Тижневих годин для денної форми навчання:
аудиторних – 3
самостійної роботи студента – 5</td><td rowspan="11">Рівень вищої освіти:
другий (магістерський)</td><td>Лекції[1)]</td></tr>
<tr><td>32 години</td></tr>
<tr><td>Практичні[1)]</td></tr>
<tr><td>0 годин</td></tr>
<tr><td>Лабораторні[1)]</td></tr>
<tr><td>16 годин</td></tr>
<tr><td>Самостійна робота</td></tr>
<tr><td>72 години</td></tr>
<tr><td>Вид контролю</td></tr>
<tr><td>Іспит</td></tr>
</table>

Співвідношення кількості годин аудиторних занять до самостійної роботи становить *48/72*.

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

2. Мета та завдання навчальної дисципліни

Мета вивчення: отримання студентами необхідних знань з науково-методичних принципів стандартизації та сертифікації продукції, а також використання їх стосовно розробки методів та засобів криптографічного захисту інформації та проектування систем захисту інформації.

Завдання:

- навчити студентів використанню вітчизняних та міжнародних стандартів при розробці систем захисту інформації;
- надати студентам знання з методів сертифиікації та оцінки якості захисту інформації;
- ознайомити студентів з базовими міжнародними стандартами в галузі забезпечення інформації;
- вивчити науково-методичні принципи стандартизації методів та засобів захисту інформації;
- вивчити призначення та основні положення базових вітчизняних та міжнародних стандартів захисту інформації;
- вивчити основні принципи та підходи до сертифікації систем, продукції та виробів в галузі захисту інформації;
- вивчити стандартні вимоги, критерії та показники ефективності функціонування систем захисту інформації та їх елементів.

Результати навчання: в результаті вивчення дисципліни студенти повинні бути здатними до:

- застосовувати методики сертифікації засобів захисту інформації;
- застосовувати стандарти при проектуванні систем захисту інформації та розробці окремих підсистем та елементів цих підсистем;
- застосовувати вимоги вітчизняних та міжнародних стандартів з сертификації та атестуваннія при сетифікації систем захисту інформації;
- здійснювати сертифікацію засобів захисту інформації на підставі методик сертификації.

Міждисциплінарні зв'язки: дисципліна базується дисципліни «Прикладна криптологія», «Комп'ютерні мережі», «Технології програмування».

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 документі 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 інформаціїї. 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 рекомнедації 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 добавленням. 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

Змістовний модуль 1. Сертифікація засобів захисту інформації. 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 нормі аудитора. Методики проведення аудиту за міжнародними та регіональними стандартами інформаційної безпеки.

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	6
Модуль 1					
Змістовий модуль 1. Науково-методичні основи стандартизації.					
Тема 1. Предмет, мета вивчення і задачі дисципліни.	6	2			4
Тема 2. Суть стандартизації та організація стандартизації в Україні.	10	6			4
Разом за змістовим модулем 1	16	8			8
Змістовий модуль 2. Методологічні основи забезпечення інформаційної безпеки.					
Тема 1. Міжнародні стандарти з основ забезпечення безпеки інформації та кібербезпеки.	26	6		6	10
Тема 2. Стандартизація механізмів кібербезпеки	40	10		6	20
Тема 3. Методи управління ключами.	26	6		6	10
Разом за змістовим модулем 2	93	22		19	52
Усього годин	113	30		19	64
Змістовий 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**..**	10	4			4
Тема 2. Основи аудиту інформаційної та кібербезпеки	12	4			6
Разом за змістовим модулем 1	22	8			10

Усього годин	**120**	**32**		**16**	**72**

5. Теми семінарських занять

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

6. Теми практичних занять

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

7. Теми лабораторних 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

8. Самостійна робота

№ з/п	Назва теми	Кількість годин
		Денна форма навчання
1	Предмет, мета вивчення і задачі дисципліни.	6
2	Суть стандартизації та організація стандартизації в Україні.	6
3	Міжнародні стандарти з основ забезпечення безпеки інформації та кібербезпеки.	12
4	Стандартизація механізмів кібербезпеки	22
5	Методи управління ключами	12
6	Основи сертифікації та ліцензування діяльності в галузі захисту	6
7	Основи аудиту інформаційної та кібербезпеки	8
	Разом	72

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 студенти

12.1. Розподіл балів, які отримують студенти (кількісні критерії оцінювання)

Складові навчальної роботи	Бали за одне заняття (завдання)	Кількість занять (завдань)	Сумарна кількість балів
Змістовий модуль 1			
Лабораторні роботи	0...10	3	0…30
Тести	0...5	1	0...5
Модульний контроль	0..10	1	0..10
Змістовий модуль 2			
Лабораторні роботи	0…10	4	0…40
Тести	0…5	1	0…5
Модульний контроль	0..10	1	0..10
Усього за семестр			**0…100**

12.2. Якісні критерії оцінювання

Необхідний обсяг знань для одержання позитивної оцінки.

1. Основи побудови і функціонування безпечних розподілених систем.
2. Класифікація, характеристики та особливості безпечних розподілених систем.
3. Особливості трафікових процесів та функцій в безпечних розподілених системах.

Необхідний обсяг умінь для одержання позитивної оцінки.

1. Уміти оптимізовувати унімодальні та багатоекстремальні трафікові функції.
2. Уміти оптимізовувати трафікові функції с декількома змінними.
3. Уміти будувати і розв’язувати лінійну модель задачі маршрутизації.
4. Уміти використовувати аналізатори трафіку, складати фільтри для аналізаторів трафіку та пояснювати отримані результати.

12.3 Критерії оцінювання роботи студента протягом семестру

1. *Задовільно (60-74)*. Мати мінімум знань і умінь. Відпрацювати та захистити всі лабораторні роботи. Знати класифікацію та характеристики мультисервісних комп’ютерних мереж та процесів, що в них протікають.
2. *Добре (75-89).* Твердо знати мінімум знань і умінь. Уміти пояснювати поведінку та властивості мультисервісних мереж. Уміти розраховувати основні характеристики мультисервісних мереж.
3. *Відмінно (90-100).* Знати всі теми. Орієнтуватися в підручниках та посібниках. Досконально знати усі функції і характеристики, класифікацію, структуризацію та характеристики сучасних високошвидкісних мультисервісних мереж. Уміти проводити розрахунок оптимальних характеристик мультисервісних мереж.

Шкала оцінювання: національна та ECTS

Сума балів за всі види навчальної діяльності	Оцінка ECTS	Оцінка за національною шкалою
90-100	**A**	відмінно
83-89	**B**	добре
75-82	**C**	
68-74	**D**	задовільно
60-67	**E**	
01-59	**FX**	незадовільно з можливістю повторного складання

13. Методичне забезпечення

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

14. Рекомендована література

Базова

1. Шаповал М.І. Основи стандартизації, управління якістю і сертифікації. – К.:2000. – 174 с.
2. Крылова Г.Д. Основы стандартизации, сертификации и метрологии. – М.:ЮНИТИ, 1999. – 711 с.
3. 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.
4. Сертифікація в України. Нормативні акти та інші документи. Т. 1,2,3. Київ, 1998.
5. Потій О.В. Конспект лекцій з дисципліни “Стандартизація та сертифікація в галузі захисту інформації”. Стандарти механізмів безпеки. –Харків, ХНУРЕ, 2001 – 80 с.
6. Потій О.В. Конспект лекцій з дисципліни “Стандартизація та сертифікація в галузі захисту інформації”. Стандарти управління ключами – Харків, ХНУРЕ, 2002 – 80 с.

Допоміжна

1. Шеннон Теория связи в секретных системах. В кн. "Труды по теории информации и кибернетики". М.: ИЛ, 1963, с.333-402.
2. Радиотехника. Всеукраинский межведомственный научно-технический сборник. Тематический выпуск «Информационная безопасность». Выпуски – 2015-2018.
3. Правове, нормативне та метрологічне забезпечення системи захисту інформації в України. Науково технічний збірник. – 2015- 2018.

15. Інформаційні ресурси

4. Міжнародні стандарти Режим доступу: https://www.iso.org/ru/home.html
5. Європейські стандарти. Режим доступу: https://www.etsi.org/standards#Security
6. Національні нормативні документи: http://www.dsszzi.gov.ua/dsszzi/control/uk/index