МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ
Тернопільський національний економічний університет

ЗАТВЕРДЖУЮ
Проректор з наукової роботи
_____ Задорожний З.-М. В.
"24" 09 2019 р.

РОБОЧА ПРОГРАМА
з дисципліни
«КІБЕРБЕЗПЕКА ІНФОРМАЦІЙНИХ І КОМП'ЮТЕРНИХ СИСТЕМ»

рівень вищої освіти – третій (освітньо-науковий)
галузь знань – 12 Інформаційні технології
спеціальність – 121 Інженерія програмного забезпечення
освітньо-наукова програма – «Інженерія програмного забезпечення»

Тернопіль – ТНЕУ
2019

СТРУКТУРА РОБОЧОЇ ПРОГРАМИ НАВЧАЛЬНОЇ ДИСЦИПЛІНИ
“Кібербезпека інформаційних і комп’ютерних систем”

Опис дисципліни “Кібербезпека інформаційних і комп’ютерних систем”

Дисципліна “Кібербезпека інформаційних і комп’ютерних систем”	**Галузь знань, спеціальність, СВО**	**Характеристика навчальної дисципліни**
Кількість кредитів – 5	Галузь знань: 12 Інформаційні технології	Статус дисципліни Обов’язкова Мова навчання: українська
Кількість залікових модулів 1	спеціальність – 121 “Інженерія програмного забезпечення”	Рік підготовки: *Денна – 1* *Заочна – 1* Семестр: *Денна – 2* *Заочна – 2, 3*
Кількість змістових модулів – 3	рівень вищої освіти – доктор філософії	Аудиторні години: *Денна – 45* *Заочна – 22*
Загальна кількість годин – 150		Самостійна робота: *Денна – 105* *Заочна – 128*
Тижневих годин: з них аудиторних: 3		Вид підсумкового контролю – екзамен

2. Мета і завдання дисципліни “Кібербезпека інформаційних і комп’ютерних систем”

2.1. Мета вивчення дисципліни.

Метою дисципліни “Кібербезпека інформаційних і комп’ютерних систем” є отримання знань та умінь, які необхідні для успішного виявлення вразливостей у комп’ютерних системах та мережах і усунення проблем безпеки шляхом розробки та впровадження захисних заходів.

2.2. Передумови для вивчення дисципліни:

Методологія наукових досліджень, Математичне моделювання та обчислювальні методи, Інформаційні технології.

2.3 Найменування та опис компетентностей, формування котрих забезпечує вивчення дисципліни:

Здатність застосовувати сучасні інформаційні технології, бази даних та інші електронні ресурси, спеціалізоване програмне забезпечення у науковій та навчальній діяльності.

2.4. Результати навчання

Розробляти та досліджувати концептуальні, математичні і комп’ютерні моделі процесів і систем, ефективно використовувати їх для отримання нових знань та/або створення інноваційних продуктів у інженерії програмного забезпечення та дотичних міждисциплінарних напрямах.

3. Зміст дисципліни “Кібербезпека інформаційних і комп’ютерних систем”

Змістовий модуль 1. Кіберпростір та кібербезпека

Тема 1. Кіберпростір, кібербезпека та кібертероризм: поняття і визначення. Кіберпростір і кібербезпека - головні ознаки нової інформаційної цивілізації. Заходи України із забезпечення кібербезпеки національної інфосфери та протидії проявам кіберзлочинності. Інциденти у сфері високих технологій: характерні ознаки та проблемні аспекти. Процедура обрання раціонального варіанта реагування на кібернетичні втручання і загрози. Особливості реалізації атак і заходи з послаблення їхнього деструктивного впливу.

Література: 1, 2, 5

Тема 2. Класифікація атак за рівнями ієрархічної моделі OSI. Атаки на фізичному рівні. Атаки на канальному рівні. Атаки на мережевому рівні.

Атаки на транспортному рівні. Атаки на рівні додатків. Загрози IP- телефонії. Аналіз віддалених мережевих служб.

Література: 1, 3, 7

Тема 3. Атаки на бездротові пристрої. Атаки на Wi-Fi. Атаки на Bluetooth. Атаки на сенсори мобільних пристроїв.

Література: 4, 5, 8

Змістовий модуль 2. Апаратні та програмні вразливості

Тема 4. Вразливості. Основні типи вразливосте й. Приклади вразливостей. Захист від вразливостей.

Література: 1, 3, 6

Тема 5. Атаки в віртуальному середовищі. Технології віртуалізації. Мережеві загрози у віртуальному середовищі. Захист віртуального середовища. Security Code vGate. Віртуальні загрози майбутнього.

Література:5, 10

Тема 6. Безпека хмарних технологій. Принцип хмари. Безпека хмарних систем. Методи шифрування в хмарних сервісах.

Література: 5, 6

Тема 7. Методи та засоби захисту інформації. Організація захисту від вірусів. Міжмережеві екрани. Засоби запобігання витокам інформації. Засоби шифрування. Одноразова аутентифікація. Honeypot - пастка для хакера.

Література: 6, 7

Тема 8. Стандарти та нормативна документація в галузі кібербезпеки. Політики безпеки. Регламент управління інцидентами.

Література: 8, 9

Змістовий модуль 3. Безпека Інтернет-речей на основі технології блокчейн

Тема 9. Безпека Інтернет речей. Концепція Інтернет-речей (IoT). Архітектура IoT. Моделі зв'язку IoT.

Література: 11, 12, 13

Тема 10. Основи технології блокчейн та приклади застосування. Принцип технології блокчейн. Структура блоку та дерево Меркле. Криптографія в блокчейн

Література: 12, 13

Тема 11. Алгоритми консенсусу в технології блокчейн. Алгоритм доказу виконання роботи (Proof-of-Work). Алгоритм підтвердження частки (Proof-of-Stake). Альтернативні алгоритми консенсусу.

Література: 12, 13

Тема 12. Безпека Інтернет-речей на основі технології блокчейн. Інтернет-речей на основі технології блокчейн. Переваги інтеграції блокчейну з IoT. Основні виклики для блокчейну в IoT. Блокчейн рішення для безпеки Інтернет-речей.

Література: 12, 13

4. Структура залікового кредиту з дисципліни "Кібербезпека інформаційних і комп'ютерних систем"

Денна форма

	Кількість годин	
	Аудиторні години	Самостійна робота
Змістовий модуль 1. Кіберпростір та кібербезпека		
Тема 1. Кіберпростір, кібербезпека та кібертероризм: поняття і визначення.	2	9
Тема 2. Класифікація атак за рівнями ієрархічної моделі OSI.	3	9
Тема 3. Атаки на бездротові пристрої.	4	9
Змістовий модуль 2. Апаратні та програні вразливості		
Тема 4. Типи вразливостей	4	9
Тема 5. Атаки в віртуальному середовищі	4	9
Тема 6 Безпека хмарних технологій	4	9
Тема 7. Методи та засоби криптографічного захисту інформації	6	9
Тема 8. Стандарти та нормативна документація в галузі кібербезпеки	2	9
Змістовий модуль 3. Безпека Інтернет-речей на основі технології блокчейн		
Тема 9. Безпека Інтернет-речей	4	9

Тема 10. Основи технології блокчейн та приклади застосування	2	8
Тема 11. Алгоритми консенсусу в технології блокчейн	4	8
Тема 12. Безпека Інтернет-речей на основі технології блокчейн	6	8
Разом	45	105

Заочна форма

	Кількість годин	
	Аудиторні години	Самостійна робота
Змістовий модуль 1. Кіберпростір та кібербезпека		
Тема 1. Кіберпростір, кібербезпека та кібертероризм: поняття і визначення.	2	10
Тема 2. Класифікація атак за рівнями ієрархічної моделі OSI.	2	10
Тема 3. Атаки на бездротові пристрої.	2	10
Змістовий модуль 2. Апаратні та програні вразливості		
Тема 4. Типи вразливостей	2	12
Тема 5. Атаки в віртуальному середовищі	2	12
Тема 6 Безпека хмарних технологій	2	10
Тема 7. Методи та засоби криптографічного захисту інформації	2	10
Тема 8. Стандарти та нормативна документація в галузі кібербезпеки	2	12
Змістовий модуль 3. Безпека Інтернет речей на основі технології блокчейн		
Тема 9. Безпека Інтернет речей	2	10
Тема 10. Основи технології блокчейн та приклади застосування	2	12
Тема 11. Алгоритми консенсусу в технології блокчейн	1	10
Тема 12. Безпека Інтернет речей на основі технології блокчейн	1	10
Разом	22	128

5. Самостійна робота

№ п/п	Тематика	К-сть годин ДФН	К-сть годин ЗФН
1	Елементи центру моніторингу та управління безпекою. SOC	4	5
2	Технології в SOC	4	5
3	Корпоративний SOC і послуги з управління інформаційною безпекою	4	5
4	Безпека кінцевих пристроїв.	5	5
5	Захист від шкідливого ПЗ на рівні хоста.	4	5
6	Захист від шкідливого ПЗ на рівні мережі.	4	5
7	Рішення для захисту від складного шкідливого програмного забезпечення Cisco AMP.	4	5
8	Міжмережеві екрани на рівні хоста.	4	5
9	Виявлення аномалій мережі	4	5
10	Перевірка мережі на уразливості	4	5
11	Загальна система оцінки вразливостей (Common Vulnerability Scoring System, CVSS).	4	5
12	База вразливостей CVE.	4	5
13	Стандарт безпеки даних індустрії платіжних карт (PCI DSS).	4	5
14	Управління ризиками.	4	5
15	Контроль вразливостей	4	5
16	Моніторинг безпеки	4	5
17	Протоколи HTTP, HTTPS, ICMP	4	5
18	Протоколи електронної пошти	4	5
19	Технології перетворення мережевих адрес (NAT) і перетворення адрес портів (PAT)	4	5
20	Реагування на інциденти і їх обробка	5	5
21	Структура правила Snort.	4	5
22	Робота в Sguil. Запити в Sguil.	4	5
23	Обробка подій в Sguil.	5	5
24	Реагування на інциденти і їх обробка	5	5

25	Життєвий цикл реагування на інциденти NIST.	5	4
26	Етапи виявлення та аналізу інцидентів.	5	4
Разом:		**105**	**128**

6. Засоби оцінювання та методи демонстрування результатів навчання

У процесі вивчення дисципліни **“Кібербезпека інформаційних і комп’ютерних систем”** використовуються наступні засоби оцінювання та методи демонстрування результатів навчання:

- стандартизовані тести;
- поточне опитування;
- командні проекти;
- аналітичні звіти, реферати, есе;
- презентації результатів виконаних завдань та досліджень;
- виступи на наукових заходах;
- завдання на лабораторному обладнанні, реальних об’єктах тощо;
- екзамен.

Шкала оцінювання:

За шкалою ТНЕУ	**За національною шкалою**	**За шкалою ECTS**
90–100	відмінно	A (відмінно)
85–89	добре	B (дуже добре)
75-84		C (добре)
65-74	задовільно	D (задовільно)
60-64		E (достатньо)
35-59	незадовільно	FX (незадовільно з можливістю повторного складання)
1-34		F (незадовільно з обов’язковим повторним курсом)

7. Інструменти, обладнання та програмне забезпечення, використання яких передбачає навчальна дисципліна

№	**Найменування**	**Номер теми**
1.	Мультимедійний проектор	1 - 12
2.	Комп’ютерна лабораторія. Доступ до Інтернету.	1 - 12

РЕКОМЕНДОВАНА ЛІТЕРАТУРА

1. Горбенко І. Д. Гриненко Т. О. Захист інформації в інформаційно-телекомунікаційних системах: Навч. посібник. Ч.1. Криптографічний захист інформації - Харків: ХНУРЕ, 2004 - 368 с.
2. Есин В. И., Кузнецов А. А., Сорока Л. С. Безопасность информационных систем и технологий – Х.:ООО «ЭДЭНА», 2010.-656с.
3. Задірака В. Компьютерная криптологія. Підручник. К, 2002 ,504с.
4. В. Столлингс. Криптография и защита сетей. Принципы и практика. Изд. “Вильямс”. К. 2001. 669 с.
5. Santos, Omar, and John Stuppi. CCNA Security 210-260 Official Cert Guide: CCNA Sec 210-260 OCG. Cisco Press, 2015.
6. Бурячок В. Л. Основи формування державної системи кібернетичної безпеки: монографія/ В. Л. Бурячок. - К.: НАУ, 2013.- 432 с.
7. Бирюков А. А. Информационная безопасность: защита и нападение. - М.: ДМК Пресс, 2012. - 474 с.
8. ISACA. Впровадження європейської кібербезпеки: настанови з управління ризиками, США, 2014 р.
9. Кузнецов О.О. Стеганографія: навч.посібн. / О.О.Кузнецов, С.П.Євсеєв, О.Г.Король. – Х.:Вид.ХНЕУ, 2011. - 232 с.
10. The Future of Wireless Networks. Architectures, Protocols, and Services. Edited by Mohesen Guizani and oth. - CRC Press, 2016 by Taylor & Francis Group. – 409 p.p.
11. James Kempf Wireless Internet Security Architecture and Protocols. - New York : Cambridge University Press, 2008. – 212 p.
12. Гепко И.А. и др. Современные беспроводные сети: состояние и перспективы развития. – К.: «ЭКМО», 2009. - 672 с.