НАЦІОНАЛЬНИЙ УНІВЕРСИТЕТ БІОРЕСУРСІВ І ПРИРОДОКОРИСТУВАННЯ УКРАЇНИ

Кафедра комп'ютерних систем, мереж та кібербезпеки

«ЗАТВЕРДЖУЮ»

Декан факультету
інформаційних технологій

проф. О.Г. Глазунова
«___» _____ 2022р.

СХВАЛЕНО
на засіданні кафедри
комп'ютерних систем,
мереж та кібербезпеки
Протокол №12 від «11» травня» 2022р.
Завідувач кафедри
(проф. Лахно В.А.)

РОЗГЛЯНУТО
Гарант ОП «Кібербезпека»

_____ (Лахно В.А.)

РОБОЧА ПРОГРАМА НАВЧАЛЬНОЇ ДИСЦИПЛІНИ «БЕЗПЕКА ТА АУДИТ БЕЗПРОВОДОВИХ ТА РУХОМИХ МЕРЕЖ»

Спеціальність	125 «Кібербезпека»
Освітня програма	«Кібербезпека»
Факультет	інформаційних технологій
Розробник:	Нікітенко Є.В., доцент, к. ф.-м. н., доцент

Київ – 2022

1. Опис навчальної дисципліни
«Безпека та аудит безпроводових та рухомих мереж»

Галузь знань, спеціальність, освітня програма, освітній ступінь		
Освітній ступінь	Бакалавр	
Галузь знань	12 – Інформаційні технології	
Спеціальність	125 – Кібербезпека	
Освітня програма	«Кібербезпека»	
Характеристика навчальної дисципліни		
Вид	обов’язкова	
Загальна кількість годин	150	
Кількість кредитів ECTS	5	
Кількість змістових модулів	3	
Курсовий проект (робота) (якщо є в робочому навчальному плані)		
Форма контролю	екзамен	
Показники навчальної дисципліни для денної та заочної форм навчання		
	денна форма навчання	заочна форма навчання
Рік підготовки	3	
Семестр	5	
Лекційні заняття, год.	30	
Практичні, семінарські заняття	-	
Лабораторні заняття, год.	30	
Самостійна робота, год.	90	
Індивідуальні завдання	-	
Кількість тижневих аудиторних годин для денної форми навчання	4	

2. Мета, завдання та компетентності навчальної дисципліни

Мета навчальної дисципліни “Безпека та аудит безпроводових та рухомих мереж” – формування у здобувачів уміння розв'язувати задачі адміністрування безпроводових і мобільних мереж і систем, застосовувати нормативно-правові, організаційні та технічні процедури при роботі безпроводових і мобільних технологій.

Вивчаються наступні теми: Безпроводові мережі загрози моделей. Безпроводовий збір даних та WiFi. MAC-аналіз. Безпроводові засоби інформаційного аналізу. Атаки на Bluetooth, DECT і ZigBee. Розширені методи атак WiFi. Захист інформації в системах мобільного зв'язку.

В результаті вивчення навчальної дисципліни студент повинен

знати:

– методи і засоби соціального інжинірингу;

– систему заходів із захисту від соціотехнічних атак;

– порядок здійснення процедур із тестування систем захисту інформації в інформаційно-комунікаційних системах на предмет проникнення, а також порядок оцінювання їхніх параметрів на різних рівнях.

вміти:

– відшукувати, збирати або добувати інформацію про ІТ-системи й мережі протиборчих сторін, а також про технології та засоби їхнього впливу на власну інфосферу;

– виявляти ознаки стороннього кібервпливу й моделювати можливі ситуації такого впливу, прогнозуючи відповідні наслідки;

– протидіяти несанкціонованому проникненню протиборчих сторін у власні ІТ-системи й мережі, забезпечуючи стійкість їхньої роботи, а також відновлення нормального функціонування після здійснення кібернападів тощо.

Відповідно до освітньої програми підготовки фахівців за спеціальністю 125 «Кібербезпека» навчальна дисципліна забезпечує формування загальних і фахових компетентностей:

Загальні компетентності:

КЗ 2. Знання та розуміння предметної області та розуміння професії.

КЗ 4. Вміння виявляти, ставити та вирішувати проблеми за професійним спрямуванням.

КЗ 8. Здатність до абстрактного і системного мислення, аналізу та синтезу.

Спеціальні (фахові) компетентності:

СК2. Здатність до використання інформаційно-комунікаційних технологій, сучасних методів і моделей інформаційної безпеки та/або кібербезпеки.

СК7. Здатність впроваджувати та забезпечувати функціонування комплексних систем захисту інформації (комплекси нормативно-правових,

організаційних та технічних засобів і методів, процедур, практичних прийомів та ін.).

СК8. Здатність здійснювати процедури управління інцидентами, проводити розслідування, надавати їм оцінку.

СК10. Здатність застосовувати методи та засоби криптографічного та технічного захисту інформації на об'єктах інформаційної діяльності.

СК12. Здатність аналізувати, виявляти та оцінювати можливі загрози, уразливості та дестабілізуючі чинники інформаційному простору та інформаційним ресурсам згідно з встановленою політикою інформаційної та/або кібербезпеки.

В результаті вивчення навчальної дисципліни студент набуде певні програмні результати, а саме

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

ПРН 26. Впроваджувати заходи та забезпечувати реалізацію процесів попередження отриманню несанкціонованого доступу і захисту інформаційних, інформаційно-телекомунікаційних (автоматизованих) систем на основі еталонної моделі взаємодії відкритих систем.

ПРН 28. Аналізувати та проводити оцінку ефективності та рівня захищеності ресурсів різних класів в інформаційних та інформаційно-телекомунікаційних (автоматизованих) системах в ході проведення випробувань згідно встановленої політики інформаційної та\або кібербезпеки.

ПРН 39. Проводити атестацію (спираючись на облік та обстеження) режимних територій (зон), приміщень тощо в умовах додержання режиму секретності із фіксуванням результатів у відповідних документах.

ПРН 41. Забезпечувати неперервність процесу ведення журналів реєстрації подій та інцидентів на основі автоматизованих процедур.

В контексті зазначених вище компетентностей та програмних результатів навчання задачі викладання дисципліни визначають необхідний комплекс знань і вмінь, що отримують студенти під час вивчення дисципліни.

Навчальна програма розрахована на студентів, які навчаються за освітньою програмою підготовки бакалавра за спеціальністю «Кібербезпека».

Програма побудована за вимогами кредитно-модульної системи організації навчального процесу у закладах вищої освіти і використанням

академічної системи оцінювання досягнень студентів та шкали оцінок Європейської кредитно-трансферної системи (ECTS).

Робоча навчальна програма з курсу «Безпека та аудит безпроводових та рухомих мереж» є основним документом, що охоплює всі види навчальної роботи при вивченні курсу студентами та відбиває основні методичні настанови кафедри.

Навчальна програма дисципліни «Безпека та аудит безпроводових та рухомих мереж» розроблена на підставі наступних документів:

- освітня програма підготовки фахівців за спеціальністю 125 «Кібербезпека»;
- навчальний план підготовки бакалаврів за спеціальністю 125 «Кібербезпека».

Навчальна програма характеризує шляхи перетворення інформації, що одержується студентом впродовж вивчання курсу, і відбиває зміст курсу, розподілення його на розділи та їх обсяги, дані про форми вивчення та контролю знань.

Теоретичною базою для вивчення курсу «Безпека та аудит безпроводових та рухомих мереж» є курс «Безпека безпровідних, мобільних та хмарних технологій».

Курс «Безпека та аудит безпроводових та рухомих мереж» є базовим для наступних дисциплін: «Комп'ютерні мережі», «Комп'ютерні системи», «Основи технічного захисту інформації».

3.Програма та структура навчальної дисципліни

– повного терміну денної (заочної) форми навчання;

Назви змістових модулів і тем	Кількість годин												
	денна форма							Заочна форма					
	тиж-ні	всього	у тому числі					всього	у тому числі				
			л	п	лр	інд	с.р.		л	п	лр	інд	с.р.
1	2	3	4	5	6	7	8	9	10	11	12	13	14
Змістовий модуль 1. Загрози для безпроводових технологій і їх аналіз													
Тема 1. Кіберпростір і кібербезпека — головні ознаки нової інформаційної цивілізації. Заходи України із забезпечення кібербезпеки національної інфосфери та протидії проявам кіберзлочинності.	1	16	3		3		10						
Тема 2. Інциденти у сфері високих технологій: характерні ознаки та проблемні аспекти. Процедура обрання раціонального варіанта реагування на кібернетичні втручання і загрози.	2	16	3		3		10						
Тема 3. Кібератаки та кібертероризм: поняття і визначення. Особливості реалізації атак і заходи з послаблення їхнього деструктивного впливу. Тип атак: зовнішні, апаратні, маскувальні. Злоякісні програмні коди.	3,4	18	4		4		10						
Разом за змістовим модулем 1		**50**	**10**		**10**		**30**						
Змістовий модуль 2. Атаки на комерційні безпроводові протоколи													
Тема 4. Бездротові мережі загрози моделей. Бездротовий збір даних та WiFi. MAC-аналіз. Бездротові засоби інформаційного аналізу	5,6	18	4		4		10						
Тема 5. Атаки на Bluetooth, DECT і ZigBee.	7	16	3		3		10						

Тема 6. Розширені методики атак WiFi.	8,9	16	3		3		10						
Разом за змістовим модулем 2		**50**	**10**		**10**		**30**						
Змістовий модуль 3. Захист інформації в системах мобільного зв'язку													
Тема 7. Засоби захисту в сучасних системах мобільного зв'язку. Соціальний фактор у проблемі забезпечення інформаційної і кібербезпеки. Загрози соціального інжинірингу. Загрози з використанням електронної пошти (e-mail). Загрози при використанні телефонного зв'язку.	10	18	4		4		10						
Тема 8. Соціальні мережі: особливості, основні поняття та визначення. Моніторинг соціальних мереж — цілі та способи реалізації.	11,12	16	3		3		10						
Тема 9. Поняття соціотехнічної системи та її властивостей. Системний підхід як загальнометодологічний принцип створення складних соціотехнічних систем.	13-15	16	3		3		10						
Разом за змістовим модулем 3		**50**	**10**		**10**		**30**						
Всього годин		**150**	**30**		**30**		**90**						

4. Теми практичних занять

№ з/п	Назва теми	Кількість годин
	Не передбачено робочим навчальним планом	

5. Теми семінарських занять

№ з/п	Назва теми	Кількість годин
	Не передбачено робочим навчальним планом	

6. Теми лабораторних занять

№ з/п	Назва теми	Кількість годин
1	Встановлення PwnPi & Kali. Безпроводова точка доступу	4
2	Встановлення дистрибутивів Linux PwnPi та Kali. Підключення до Raspberry Pi через SSH і VNC. Налаштовування DHCP та DNS сервісів. Запуск програмної точки доступу на Raspberry Pi	2
3	Розробка карти безпроводової мережі. Побудова діаграми зв'язку «клієнт-точка доступу» та «клієнт-зонд»	4
4	Використання GPS-модуля у безпроводовому мережевому скануванні	4
5	Аналіз результатів airodump-ng та експорт у JSON. Розробка GPS-маршруту на Google-картах.	4
6	Моніторинг мережевого трафіку	2
7	Технології злому WEP та WPS. Перевірка точки доступу на уразливість WEP та WPS	4
8	DoS-атаки на Wi-Fi мережі	2
9	Тестування випадковими даними безпроводової точки доступу та проведення часткового аналізу безпеки за стандартом PCI DSS, який відповідає за безпроводову мережу	4
	Всього	30

САМОСТІЙНА РОБОТА СТУДЕНТІВ

Самостійна робота студентів передбачає:

- систематичне відвідання усіх видів аудиторних занять і ведення конспекту лекцій;
- систематичне вивчення лекційного матеріалу і навчальної літератури, що рекомендуються;
- сумлінну підготовку до лабораторних занять;
- вчасне і якісне оформлення звітів про лабораторні роботи.

7. Контрольні питання, комплекти тестів для визначення рівня засвоєння знань студентами

7.1. Питання для перевірки знань студентів:

1. Кіберпростір і кібербезпека — головні ознаки нової інформаційної цивілізації.
2. Заходи України із забезпечення кібербезпеки національної інфосфери та протидії проявам кіберзлочинності.

3. Дайте визначення понять інформаційний простір і кібернетичний простір. Назвіть основних дійових осіб кіберпростору.
4. Інциденти у сфері високих технологій: характерні ознаки та проблемні аспекти.
5. Процедура обрання раціонального варіанта реагування на кібернетичні втручання і загрози.
6. Що таке кібероборотьба? Які основні особливості їй притаманні?
7. Дайте визначення поняття інформаційна безпека. Назвіть основні чинники, які на неї негативно впливають, та методи, завдяки яким цьому можна запобігти.
8. Дайте визначення поняття кібернетична безпека. Назвіть істотні ознаки, які його характеризують.
9. Кібератаки та кібертероризм: поняття і визначення.
10. Особливості реалізації атак і заходи з послаблення їхнього деструктивного впливу.
11. Тип атак: зовнішні, апаратні, маскувальні.
12. Злоякісні програмні коди.
13. Які документи регламентують діяльність із забезпечення інформаційної та кібернетичної безпеки в Україні? Наведіть приклади внеску в реалізацію цих процесів державних підрозділів спецпризначення.
14. Дайте визначення понять кібервтручання і кіберзагроза.
15. Що слід розуміти під поняттям інциденту у сфері високих технологій? Розкрийте сутність процесу управління інцидентами.
16. Опишіть модель системи управління інцидентами та розкрийте сутність її складових.
17. Дайте визначення внутрішнього і зовнішнього інциденту. Наведіть приклади таких інцидентів класифікації згідно з кодифікатором Інтерполу.
18. Які з вдомих інцидентів становлять нині найбільшу небезпеку?
19. Наведіть приклади деструктивних інцидентів у сфері високих технологій. Розкрийте відмітні риси мережних черв'яків Stuxnet, Duqu та Flame.
20. Назвіть найбільш критичні заходи захисту інформації від кіберзагроз.
21. Перелічіть основні кроки, які мають бути дотримані співробітниками служб безпеки в разі фіксації порушень інформаційної та кібернетичної безпеки.
22. Дайте визначення поняття кібератака. Наведіть приклади його тлумачення різними категоріями дослідників.
23. За якими основними ознаками кібератаки можуть бути класифіковані?
24. Назвіть основні типи кібератак за класифікацією П. Ноймана.
25. Наведіть приклад алгоритму реалізації кібератак.
26. Дайте визначення поняття кібертероризм. Наведіть приклади його тлумачення різними категоріями дослідників.
27. Назвіть основні риси кібертероризму. Що сприяє сучасним терористам у веденні їх протиправної діяльності та забезпечує їм успіх?

28. Назвіть головні прийоми, якими користуються сучасні кібертерористи у процесі своєї протиправної діяльності.
29. Які чинники впливають на поширення кібертероризму в Україні?
30. Що таке сніфер пакетів? Які заходи сприятимуть зниженню загрози сніфінгу?
31. Що таке IP-спуфінг? Завдяки чому можна послабити загрозу IP-спуфінгу?
32. Що таке DoS та DDoS атаки? Назвіть найбільш відомі їх різновиди.
33. За рахунок чого можна послабити загрози від DoS та DDoS атак?
34. Бездротові мережі загрози моделей.
35. Бездротовий збір даних та WiFi. MAC-аналіз.
36. Бездротові засоби інформаційного аналізу.
37. Атаки на Bluetooth, DECT і ZigBee.
38. Розширені методики атак WiFi.
39. Засоби захисту в сучасних системах мобільного зв'язку.
40. Соціальний фактор у проблемі забезпечення інформаційної і кібербезпеки.
41. Загрози соціального інжинірингу.
42. Загрози з використанням електронної пошти (e-mail).
43. Загрози при використанні телефонного зв'язку.
44. Соціальні мережі: особливості, основні поняття та визначення.
45. Моніторинг соціальних мереж.
46. Поняття соціотехнічної системи та її властивостей.
47. Системний підхід як загальнометодологічний принцип створення складних соціотехнічних систем.

8. Методи навчання

Пояснювально-ілюстративний метод – застосовується в ході лекцій та у процесі самостійної роботи студентів для передачі великих масивів навчальної інформації в опрацьованому вигляді.

Репродуктивний метод – застосовується в ході лабораторних занять і процесі самостійної роботи, передбачає набуття студентами навичок використання визначених алгоритмів вирішення навчальних та професійних завдань.

Метод проблематизації та евристичний метод – застосовуються в ході лекційних, лабораторних занять, самостійної та індивідуальної роботи.

9. Форми контролю

Систематичний контроль за самостійною роботою студентів і якістю засвоєння ними поточного навчального матеріалу:

- на лабораторних роботах шляхом перевірки підготовки до виконання роботи;
- роботу над індивідуальними завданнями до лабораторних робіт;
- вивчення літератури, що рекомендувалася, та конспекту лекцій;
- оформлення звітів про виконання лабораторним роботам.

Поточний контроль знань студентів проводиться:

- на лабораторних роботах оцінюється підготовка до роботи, обсяг її виконання, результати захисту звіту;
- на лекційних заняттях виконується вибіркове опитування студентів;
- шляхом проведення модульних контролів знань студентів та виставлення рейтингових оцінок знань студентів по усім видам занять.

10. Розподіл балів, які отримують студенти

Оцінювання знань студента відбувається за 100-бальною шкалою і переводиться в національні оцінки згідно з табл.1 «Положення про екзамени та заліки у НУБіП України» (наказ про уведення в дію від 27.12.2019р. № 1371):

Рейтинг здобувача вищої освіти, бали	**Оцінка національна за результати складання екзаменів заліків**	
	Екзамен	**Залік**
90-100	Відмінно	зараховано
74-89	Добре	
60-73	Задовільно	
0-59	незадовільно	не зараховано

Для визначення рейтингу студента із засвоєння дисципліни $R_{дис}$ (до 100 балів) одержаний рейтинг з атестації $R_{АТ}$ (до 30 балів) додається до рейтингу студента з навчальної роботи $R_{НР}$ (до 70 балів): $R_{дис}=R_{НР}+R_{АТ}$.

11. Рекомендована література

основна:

1. Бурячок В. Л. Основи інформаційної та кібернетичної безпеки. [Навчальний посібник]. / В. Л. Бурячок , Р. В. Киричок, П. М. Складанний – К. , 2018. – 320 с.
2. Бурячок В. Л., Соколов В. Ю. Методи забезпечення гарантоздатності і функціональної безпеки безпроводової інфраструктури на основі апаратного розділення абонен-тів : Монографія. Київ : КУБГ, 2019. 164 с.
3. Соколов, В. Ю. Безпека безпроводових і мобільних мереж : Навчальний посібник / В. Ю. Соколов, В. Л. Бурячок, М. М. Тадждіні / ред. перекл. О. П. Райтер. — 2 вид., доп. — К. : КУБГ, 2019. — 130 с.
4. Ахрамович В.М. Курс лекцій з навчальної дисципліни «Кібербезпека банківських та комерційних структур» /В.М.Ахрамович. Державний університет телекомунікацій. – К.:ДУТ, 2019. – 163 с. іл. – Бібліограф.: 166 с.
5. Безпека електронної комерції: навч. посібн. І.М. Пістунов, Є.В., Кочура; Нац. гірн. ун–т. Дніпропетровськ: НГУ, 2014. 125 с.
6. Основи інформаційної безпеки / Андрєєв В. І. та ін. ; за ред. В. О. Хорошка. 2-е вид. Київ, 2009. 292 с.

допоміжна:

1. НД ТЗІ 2.5-004-99. Критерії оцінки захищеності інформації в комп’ютерних системах від несанкціонованого доступу. Київ : Департамент спеціальних телекомунікаційних систем та захисту інформації, 1999. 53 с. (Служба безпеки України).