НАЦІОНАЛЬНИЙ УНІВЕРСИТЕТ БІОРЕСУРСІВ І ПРИРОДОКОРИСТУВАННЯ УКРАЇНИ

Кафедра комп'ютерних систем, мереж та кібербезпеки

"ЗАТВЕРДЖУЮ"
Декан факультету інформаційних технологій
_____ проф. О.Г. Глазунова
"__" _____ 2023 р.

СХВАЛЕНО
на засіданні кафедри
комп'ютерних систем, мереж та кібербезпеки
Протокол №10 від "17" травня 2023 р.
Завідувач кафедри
(доц. Касаткін Д.Ю.)

РОЗГЛЯНУТО
Гарант ОП
«Кібербезпека»
_____
Гарант ОП
_____ (проф. Лахно В.А.)

РОБОЧА ПРОГРАМА НАВЧАЛЬНОЇ ДИСЦИПЛІНИ «БЕЗПЕКА БЕЗПРОВІДНИХ, МОБІЛЬНИХ ТА ХМАРНИХ ТЕХНОЛОГІЙ»

Спеціальність	125 «Кібербезпека»
Освітня програма	«Кібербезпека»
Факультет	інформаційних технологій
Розробник:	Лахно В.А., д.т.н., проф.

Київ – 2023

Опис навчальної дисципліни
«Безпека безпровідних, мобільних та хмарних технологій»

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	120	
Кількість кредитів ECTS	4	
Кількість змістових модулів	2	
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	2	
Семестр	4	
Лекційні заняття, год.	30	
Практичні, семінарські заняття	-	
Лабораторні заняття, год.	30	
Самостійна робота, год.	60	
Індивідуальні завдання	-	
Кількість тижневих аудиторних годин для денної форми навчання	4	

1. Мета, завдання та компетентності навчальної дисципліни

Мета: формування теоретичних знань і придбання практичних умінь і навичок з питань використання технологій захищених розподілених обчислень, віртуалізації серверних систем, проектування захищених корпоративних обчислювальних систем із застосуванням безпровідних, мобільних і хмарних обчислень.

Завдання навчальної дисципліни: є теоретична та практична підготовка студентів до застосування використання технологій захищених розподілених обчислень, віртуалізації серверних систем, проектування захищених корпоративних обчислювальних систем із застосуванням безпровідних, мобільних і хмарних обчислень.

В результаті вивчення навчальної дисципліни студент повинен

- знати: основні поняття технологій захищених розподілених обчислень, віртуалізації серверних систем, проектування захищених корпоративних обчислювальних систем із застосуванням безпровідних, мобільних і хмарних обчислень; бездротові технології та їх протоколи; класифікацію загроз та вразливостей мобільних додатків, мобільних пристроїв; мережеві протоколи та служби; мережеву інфраструктура для бездротових мереж; класифікацію загроз та вразливостей Wi-Fi-мереж, їх захист; хмарні технології та основи побудови інфраструктури; принципи забезпечення безпеки у бездротових мережах; принципи моніторингу безпеки бездротових мереж; підходи до захисту від мережевих атак; методи забезпечення безпеки інформації у хмарних сервісах; основи криптографії та інфраструктуру загальних ключів; засоби віртуалізації, принципи роботи та засоби захисту, системи реагування на інциденти інформаційної безпеки.

- вміти:

здійснювати документування подій у мережі, автоматизацію записів; здійснювати класифікацію мережевих атак, застосовувати методи протидії таким атакам; застосовувати методи захисту даних у хмарних технологіях; використовувати методи хешування, шифрування та захищені з’єднання; застосування систем реагування на інциденти інформаційної безпеки; здійснювати моніторинг та спеціалізовану структуру керування безпекою; аналізувати та досліджувати загрози та вразливості мобільних додатків та мобільних пристроїв; вирішувати задачу побудови безпечної бездротової мережі на основі різних пристроїв та технологій; досліджувати загрози та вразливості WiFi-мереж; вирішувати задачу побудови безпечної хмарної інфраструктури.

Набуття компетентностей:

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

Загальні компетентності:

ЗК1. Здатність застосовувати знання у практичних ситуаціях.

ЗК2. Знання та розуміння предметної області та розуміння професії.

ЗК4. Вміння виявляти, ставити та вирішувати проблеми за професійним спрямуванням.

Спеціальні (фахові, предметні) компетентності (СК):

СК1. Здатність застосовувати законодавчу та нормативно-правову базу, а також державні та міжнародні вимоги, практики і стандарти з метою здійснення професійної діяльності в галузі інформаційної та/або кібербезпеки.

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

СК3. Здатність до використання програмних та програмно-апаратних комплексів засобів захисту інформації в інформаційно-телекомунікаційних (автоматизованих) системах.

СК5. Здатність забезпечувати захист інформації, що обробляється в інформаційно-телекомунікаційних (автоматизованих) системах з метою реалізації встановленої політики інформаційної та/або кібербезпеки.

СК6. Здатність відновлювати штатне функціонування інформаційних, інформаційно-телекомунікаційних (автоматизованих) систем після реалізації загроз, здійснення кібератак, збоїв та відмов різних класів та походження.

СК7. Здатність впроваджувати та забезпечувати функціонування комплексних систем захисту інформації (комплекси нормативно-правових, організаційних та технічних засобів і методів, процедур, практичних прийомів та ін.).

СК9. Здатність здійснювати професійну діяльність на основі впровадженої системи управління інформаційною та/або кібербезпекою.

СК11. Здатність виконувати моніторинг процесів функціонування інформаційних, інформаційно-телекомунікаційних (автоматизованих) систем згідно встановленої політики інформаційної та/або кібербезпеки.

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 (РН), а саме

РН11. Виконувати аналіз зв’язків між інформаційними процесами на віддалених обчислювальних системах.

РН13. Аналізувати проекти інформаційно-телекомунікаційних систем, базуючись на стандартизованих технологіях та протоколах передачі даних.

РН14. Вирішувати завдання захисту програм та інформації, що обробляється в інформаційно-телекомунікаційних системах програмно-апаратними засобами та давати оцінку результативності якості прийнятих рішень.

РН17. 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.

РН25. Забезпечувати введення підзвітності системи управління доступом до електронних інформаційних ресурсів і процесів в інформаційних та інформаційно-телекомунікаційних (автоматизованих) системах з використанням журналів реєстрації подій, їх аналізу та встановлених процедур захисту.

РН27. Вирішувати задачі захисту потоків даних в інформаційних, інформаційно-телекомунікаційних (автоматизованих) системах.

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 безпровідних, мобільних та хмарних технологій» є основним документом, що охоплює всі види навчальної роботи при вивченні курсу студентами та відбиває основні методичні настанови кафедри.

Навчальна програма дисципліни «Безпека безпровідних, мобільних та хмарних технологій» розроблена на підставі наступних документів:

- освітня програма підготовки фахівців за спеціальністю 125 «Кібербезпека»;
- навчальний план підготовки фахівців 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 безпровідних, мобільних та хмарних технологій» є курси «Організаційне забезпечення захисту інформації» та «Методи та засоби захисту інформації».

Курс «Безпека безпровідних, мобільних та хмарних технологій» є базовим для вивчення наступної дисципліни: «Технології безпечного програмування».

2.Програма та структура навчальної дисципліни

– повного терміну денної (заочної) форми навчання;

Назви змістових модулів і тем	Кількість годин												
	денна форма							Заочна форма					
	тиж-ні	всьо-го	у тому числі					всьо-го	у тому числі				
			л	п	лр	ін д	с.р.		л	п	лр	ін д	с.р.
1	2	3	4	5	6	7	8	9	10	11	12	13	14
Змістовий модуль 1. Концепція динамічної маршрутизації.													
Тема 1. Центр моніторингу та керування безпекою.	1	8	2		2		4						
Тема 2. Бездротові технології та їх протоколи.	2	8	2		2		4						
Тема 3. Загрози та вразливості мобільних додатків, мобільних пристроїв (Ч1).	3	8	2		2		4						
Тема 4. Загрози та вразливості мобільних додатків, мобільних пристроїв (Ч2).	4	8	2		2		4						
Тема 5. Мережеві протоколи та служби.	5	8	2		2		4						
Тема 6. Мережева інфраструктура для бездротових мереж.	6	8	2		2		4						
Тема 7. Загрози та вразливості Wi-Fi-мереж та їх захист.	7	8	2		2		4						
Тема 8. Хмарні технології та основи побудови інфраструктури.	8	8	2		2		4						
Разом за змістовим модулем 1		**64**	**16**		**16**		**32**						
Змістовий модуль 2 Забезпечення безпровідних, мобільних та хмарних технологій.													
Тема 1. Принципи забезпечення безпеки у бездротових мережах. Моніторинг безпеки бездротових мереж (Ч1).	9	8	2		2		4						
Тема 2. Принципи забезпечення безпеки у бездротових мережах. Моніторинг безпеки бездротових мереж (Ч2).	10	8	2		2		4						

Тема 3. Захист від мережевих атак.	11	8	2		2		4						
Тема 4. Забезпечення безпеки інформації у хмарних сервісах.	12	8	2		2		4						
Тема 5. Криптографія та інфраструктура відкритих ключів.	13	8	2		2		4						
Тема 6. Засоби віртуалізації. Типи. Принципи роботи. Засоби захисту.	14	8	2		2		4						
Тема 7. Реагування на інциденти та їх обробка.	15	8	2		2		4						
Разом за змістовим модулем 2		**56**	**14**		**14**		**28**						
Всього годин		**120**	**30**		**30**		**60**						

3. Теми практичних занять

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

Теми семінарських занять

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

4. Теми лабораторних занять

№ з/п	Назва теми	Кількість годин
1	Введення в основи моніторингу та спеціалізованих структур керування безпекою.	2
2	Дослідження бездротових технологій та їх протоколів.	2
3	Аналіз та дослідження загроз та вразливостей мобільних додатків та мобільних пристроїв.	4
4	Вивчення основних мережевих протоколів та принципів їх роботи.	2
5	Основи побудови бездротової мережі на основі різних пристроїв та технологій.	2
6	Дослідження загроз та вразливостей WiFi-мереж.	2
7	Дослідження побудови хмарної інфраструктури.	2
8	Дослідження документування подій у мережі, автоматизація записів.	4
9	Дослідження класифікації мережевих атак та дослідження методів протидії і захисту.	2

10	Дослідження моделей обслуговування у хмарних технологіях.	2
11	Дослідження методів хешування, шифрування, видів ключів та захищених з’єднань.	2
12	Дослідження засобів віртуалізації та принципів їх роботи.	2
13	Дослідження систем реагування на інциденти інформаційної безпеки.	2
	Всього	30

Курсове проектування - Не передбачено робочим навчальним планом

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.

Теми самостійної роботи

№ з/п	Назва теми	Кількість годин
1	Основні мережеві протоколи та принципи їх роботи.	6
2	Побудова бездротової мережі на основі різних пристроїв та технологій.	6
3	Вразливості WiFi-мереж.	6
4	Побудова хмарної інфраструктури.	6
5	Документування подій у мережі, автоматизація записів.	6
6	Класифікації мережевих атак та дослідження методів протидії і захисту.	6
7	Моделі обслуговування у хмарних технологіях.	6
8	Методи хешування, шифрування, види ключів та захищених з’єднань.	6
9	Засобів віртуалізації та принципів їх роботи.	6
10	Системи реагування на інциденти інформаційної безпеки.	6
	Всього	60

Контрольні питання, комплекти тестів для визначення рівня засвоєння знань студентами

1.1. Питання для перевірки знань студентів:

1. Поняття центру моніторингу та керування безпекою.
2. Бездротові технології.

3. Протоколи бездротових технологій.
4. Загрози та вразливості мобільних додатків.
5. Загрози та вразливості мобільних пристроїв.
6. Мережеві протоколи та служби.
7. Мережева інфраструктура для бездротових мереж.
8. Загрози Wi-Fi-мереж.
9. Вразливості Wi-Fi-мереж.
10. Захист Wi-Fi-мереж.
11. Поняття хмарних технологій.
12. Підходи до забезпечення безпеки інформації у хмарних сервісах.
13. Основи побудови інфраструктури хмарних технологій.
14. Принципи забезпечення безпеки у бездротових мережах.
15. Моніторинг безпеки бездротових мереж.
16. Типи мережевих атак.
17. Методи захисту від мережевих атак.
18. Технології аутентифікації.
19. Протоколи захисту канального рівня.
20. Протоколи захисту сеансового рівня.
21. Методи захисту на мережевому рівні.
22. Технології міжмережевого екранування.
23. Технології віртуальних захищених мереж.
24. Інфраструктура захисту на прикладному рівні.
25. Методи хешування.
26. Методи шифрування.
27. Інфраструктура відкритих ключів.
28. Системи реагування на інциденти інформаційної безпеки.
29. Сутність інфраструктури як послуги.
30. Сутність програмного забезпечення як послуги.
31. Сутність платформи як послуги.
32. Загрози конфіденційності хмари.

1.2. Приклади тестів з дисципліни:

1. Інфраструктура як сервіс - це ...

А) надання комп'ютерної інфраструктури, як послуги, на основі концепції хмарних обчислень;

В) надання інтегрованої платформи для розробки, тестування, розгортання і підтримки веб-додатків як послуги;

С) модель розгортання програми, за допомогою якої надаються додатки кінцевому користувачеві як послуги на вимогу.

2. Система зберігання даних - це ...

А) головний комп'ютер обчислювального центру з великим об'ємом внутрішньої і зовнішньої пам'яті;

В) програмно-апаратне рішення по організації надійного зберігання інформаційних ресурсів та надання до них гарантованого доступу;

С) об'єднання обчислювальних ресурсів або структур управління в єдиному центрі.

2. Методи навчання

Виконання лабораторних робіт з використанням ПЗ WEKA; виконання індивідуальних навчально-дослідних завдань.

3. 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.

4. 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 «26» квітня 2023 р. протокол № 10):

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): $R_{дис}=R_{НР}+R_{АТ}$.

5. Методичне забезпечення

1. Електронний навчальний курс на платформі Moodle вміщує повне методичне забезпечення включаючи: лекції, презентації до лекцій, методичні вказівки до виконання лабораторних робіт, глосарій термінів тощо.

6. Рекомендовані джерела інформації

1. Зінченко О.В., Іщеряков С.М., Прокопов С.В., Сєрих С.О., Василенко В.В. Хмарні технології. – Навчальний посібник. – К: ФОП Гуляєва В.М., 2020. – 74 с.

2. Соколов В. Ю. Безпека безпроводових і мобільних мереж: Навчальний посібник / В. Ю. Соколов, В. Л. Бурячок, М. М. Таджділні / ред. перекл. О. П. Райтер. — 2 вид., доп. — К. : КУБГ, 2019. — 130 с.

3. Raghuram Yeluri, Enrique Castro-Leon. Building the Infrastructure for Cloud Security: A Solutions View. Apress, 2014 p. - 244 p.

4. Huseni Saboowala, Muhammad Abid, Sudhir Modali. Designing Networks and Services for the Cloud: Delivering business-grade cloud applications and services. Cisco Press, 2013. - 336 p.

Інформаційні ресурси

1. АДМІНІСТРАЦІЯ ДЕРЖАВНОЇ СЛУЖБИ СПЕЦІАЛЬНОГО ЗВ'ЯЗКУ ТА ЗАХИСТУ ІНФОРМАЦІЇ УКРАЇНИ [Електронний ресурс] – Режим доступу: http://www.dsszzi.gov.ua/dsszzi/control/uk/publish/article?art_id=81998&cat_id=38835