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 ПРИ ЕКСПЛУАТАЦІЇ І ОБСЛУГОВУВАННІ ІТ СИСТЕМ

спеціальність	125 "Кібербезпека"
освітня програма	Кібербезпека
Факультет	Інформаційних технологій
Розробник:	Дрейс Ю.О., к.т.н., доцент

Київ – 2022 р.

1. Опис навчальної дисципліни

БЕЗПЕКА ПРИ ЕКСПЛУАТАЦІЇ І ОБСЛУГОВУВАННІ ІТ СИСТЕМ

Галузь знань, спеціальність, освітня програма, освітній ступінь		
Освітній ступінь	Бакалавр	
Спеціальність	125 – Кібербезпека	
Освітня програма	Кібербезпека	
Характеристика навчальної дисципліни		
Вид	Вибіркова	
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 (курс)	4	
Семестр	7	
Лекційні заняття	30	
Практичні, семінарські заняття	–	
Лабораторні заняття	30	
Самостійна робота	60	
Індивідуальні завдання	–	
Кількість тижневих аудиторних годин для денної форми навчання	3	

2. Мета та завдання навчальної дисципліни

Метою викладання дисципліни є формування теоретичних знань та практичних навичок, необхідних для ефективного та безпечного використання інформаційних технологій в інформаційних системах підприємств АПК і мережах а також запобігання розголошенню, витоку і неправомірному оволодінню інформацією, протиправним діям щодо знищення, модифікації, копіювання і блокування інформації..

Навчальна дисципліна забезпечує формування ряду фахових компетентностей:

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.

СК4. Здатність забезпечувати неперервність бізнесу згідно встановленої політики інформаційної та/або кібербезпеки.

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.

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

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

СК11. Здатність виконувати моніторинг процесів функціонування інформаційних, інформаційно-телекомунікаційних (автоматизованих) систем згідно

встановленої політики інформаційної та/або кібербезпеки.

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

ПРН 14. Вирішувати завдання захисту програм та інформації, що обробляється в інформаційно-телекомунікаційних системах програмно-апаратними засобами та давати оцінку результативності якості прийнятих рішень;

ПРН 17. 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;

ПРН 20. Забезпечувати функціонування спеціального програмного забезпечення, щодо захисту інформації від руйнуючих програмних впливів, руйнуючих кодів в інформаційно-телекомунікаційних системах;

ПРН 21. Вирішувати задачі забезпечення та супроводу (в.т. числі: огляд, тестування, підзвітність) системи управління доступом згідно встановленої політики безпеки в інформаційних та інформаційно-телекомунікаційних (автоматизованих) системах;

ПРН 36. Виявляти небезпечні сигнали технічних засобів;

ПРН 37. Вимірювати параметри небезпечних та завадових сигналів під час інструментального контролю процесів захисту інформації та визначати ефективність захисту інформації від витоку технічними каналами відповідно до вимог нормативних документів системи технічного захисту інформації;

ПРН 38. Інтерпретувати результати проведення спеціальних вимірювань з використанням технічних засобів, контролю характеристик інформаційно-телекомунікаційних систем відповідно до вимог нормативних документів системи технічного захисту інформації;

ПРН 40. Інтерпретувати результати проведення спеціальних вимірювань з використанням технічних засобів, контролю характеристик ІТС відповідно до вимог нормативних документів системи технічного захисту інформації;

ПРН 49. Забезпечувати належне функціонування системи моніторингу інформаційних ресурсів і процесів в інформаційно-телекомунікаційних системах;

ПРН 50. Забезпечувати) функціонування програмних та програмно-апаратних комплексів виявлення вторгнень різних рівнів та класів (статистичних, сигнатурних, статистично-сигнатурних);

ПРН 51. Підтримувати працездатність та забезпечувати конфігурування систем виявлення вторгнень в інформаційно-телекомунікаційних системах.

3. Програма та структура навчальної дисципліни

Назви змістових модулів і тем	Кількість годин												
	денна форма							Заочна форма					
	тижні	усього	у тому числі					усього	у тому числі				
			л	п	лаб	інд	с.р.		л	п	лаб	інд	с.р.
1	2	3	4	5	6	7	8	9	10	11	12	13	14
Семестр 5													
Модуль 1.													
Шкідливе програмне забезпечення і захист від руйнуючих програмних дій.	1	7	2				5						
Адміністративне та організаційне забезпечення інформаційно-телекомунікаційних систем підприємств АПК.	1	9	2		2		5						
Інженерно–технічне забезпечення інформаційно-телекомунікаційних систем підприємств АПК.	2	16	2		4		10						
Апаратні та програмні засоби захисту підприємств АПК.	2	18	4		4		10						
Разом за змістовим модулем 1	**50**		**10**		**10**		**30**						
Модуль 2.													
Технології безпеки на основі фільтрації та моніторингу мережевого трафіку.	1	14	4		4		6						
Основи криптографічного захисту інформації.	2	14	4		4		6						
Протоколи захисту в телекомунікаційних мережах.	2	14	4		4		6						
Безпечна робота в комп'ютерних мережах.	2	14	4		4		6						
Безпека при експлуатації і обслуговуванні іт систем підприємств АПК.	2	14	4		4		6						
Разом за змістовим модулем 2	70		20		20		30						
Всього за семестр	**120**		**30**		**30**		**60**						
Усього годин	**120**												

4. Теми семінарських занять

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

5. Теми практичних занять

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

6. Теми лабораторних занять

№ з/п	Назва теми	Кількість годин
1	Побудова схеми управлінського моніторингу ІКС.	4
2	Планування заході що до впровадження механізмів реалізації послуг безпеки (зокрема, на прикладі підприємств АПК).	6
3	Аналіз моделей безпеки ІКС для конкретного ОБІ (зокрема, на прикладі підприємств АПК).	4
4	Аналіз безпеки програмного забезпечення для ОБІ (зокрема, на прикладі підприємств АПК).	4
5	Побудова концептуальної моделі архітектури безпеки ІКС ОБІ.	4
6	Планування методів захисту інформації в ІКС, зокрема, на прикладі підприємств АПК.	4
7	Автентифікація користувачів у ІКС ОБІ.	4
	Усього годин	**30**

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

Питання для перевірки знань студентів:

1. Механізми реалізації послуг безпеки.
2. Побудова та впровадження СЗІ.
3. Механізми і політики розмежування прав доступу в ІКС.
4. Засоби забезпечення захисту інформації в ІКС.
5. Засоби ідентифікації й автентифікації об’єктів баз даних, управління доступом.
6. Засобу контролю цілісності інформації, організація аудиту.
7. Види загроз для інформаційної безпеки (ІБ).
8. Рольова політика безпеки.
9. Монітор безпеки.
10. Методи аналізу безпеки ПЗ.
11. Нелегітимне використання ресурсів.
12. Нелегітимний доступ до даних.
13. Нелегітимний запуск програм.
14. Нелегітимне виконання програм.
15. Нелегітимна відмова в обслуговування (порушення доступності).
16. Тенденції розвитку систем захисту ІТКС.
17. Класи атак.
18. Захист шлюзів.
19. Міжмережеві екрани.
20. Розробка конфігурації міжмережевих екранів.
21. Інструментальні та прикладні застосунки в інформаційній та/або кібербезпеці.
22. Мережева модель OSI. Основні протоколи стеку TCP/IP.
23. Віртуалізація (принципи, гіпервізори).

24. Захисні механізми операційних систем.
25. Моделі безпеки в інформаційній та/або кібербезпеці.
26. Процедури ідентифікації, автентифікації, авторизації користувачів.
27. Резервування інформації та компонентів ІКС.
28. Програмні та програмно-апаратні комплекси ЗЗІ.
29. Антивіруси, міжмережеві екрани.
30. Системи відеоспостереження.

8. Методи навчання

Бесіда, співбесіда, пояснення, інноваційні методи з використанням мультимедійних презентацій.

9. Форми контролю

Опитування
Захист лабораторної роботи, теми.
Реферативні повідомлення
Модульне тестування.
Екзамен

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 27.12.2019 р. № 1371)

Рейтинг студента, бали	**Оцінка національна за результати складання**	
	екзаменів	**заліків**
90-100	**Відмінно**	**Зараховано**
74-89	**Добре**	
60-73	**Задовільно**	
0-59	**Незадовільно**	**Не зараховано**

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

11. Рекомендована література

1. Грайворонський М.В.,. Новіков О.М Безпека інформаційно-комунікаційних систем. – К.: Видавнича група BHV, 2009. – 608 с.
2. Остапов С.Е., Євсеєв С.П., Король О.Г., Технології захисту інформації. Навчальний посібник. Чернівці.- Видавничий дім «Родовід», 2014. – 471с.
3. Кавун С.В. Інформаційна безпека: підручник. Харків : ХНЕУ, 2013. -213с.
4. Гончарова Л.Л., Возненко А.Д., Стасюк О.І., Коваль Ю.О. Основи захисту інформації в телекомунікаційних та комп'ютерних мережах: навч. посібник. – К., 2013. – 435с., іл.160.
5. Єсін В. І. Безпека інформаційних систем і технологій: навчальний посібник / В. І. Єсін, О. О. Кузнецов, Л. С. Сорока. – Х. : ХНУ імені В. Н. Каразіна, 2013. – 632с

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