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 ІНФОРМАЦІЇ В ІНФОРМАЦІЙНО-КОМУНІКАЦІЙНИХ СИСТЕМАХ»

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

Київ – 2023

1. Опис навчальної дисципліни «Безпека інформації в інформаційно-комунікаційних системах»

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	3	
Семестр	5	
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	

2. Мета, завдання та компетентності навчальної дисципліни

Мета: розкриття сучасних методів захисту інформації в інформаційно-комунікаційних системах. Дисципліна передбачає вивчення: видів загроз інформації в інформаційно-комунікаційних системах; програмних та програмно-апаратних комплексів засобів захисту інформації; відновлення функціонування інформаційно-комунікаційних систем після реалізації загроз, здійснення кібератак, збоїв та відмов; моніторинг процесів функціонування інформаційно-комунікаційних систем; механізми безпеки комп'ютерних мереж.

Завдання навчальної дисципліни: є теоретична та практична підготовка студентів щодо вирішення професійних задач, що базуються на сучасних технологіях та методах захисту інформації у сучасних інформаційно-комунікаційних систем та мережах.

В результаті вивчення навчальної дисципліни студент повинен

- знати: процеси захисту інформаційно-комунікаційних систем від порушників безпеки інформації; методи та види несанкціонованого доступу та канали витоку інформації в інформаційно-комунікаційних системах; методику визначення необхідного рівня захищеності інформації в інформаційно-комунікаційних системах; принципи протидії несанкціонованому доступу до ресурсів і процесів в інформаційно-комунікаційних системах; функції та особливості реалізації системи захисту інформації в інформаційно-комунікаційних системах

- вміти:

вирішувати задачі супроводу та впровадження систем захисту інформації в інформаційно-комунікаційних системах, а також протидії несанкціонованому доступу до ресурсів і процесів в інформаційних та інформаційно-комунікаційних системах; здійснювати оцінку рівня захищеності інформації що обробляється в інформаційно-комунікаційних системах використовувати інструментальні засоби оцінювання; готувати пропозиції до нормативних актів і документів з метою забезпечення встановленої політики інформаційної безпеки і \або кібербезпеки; розробляти проектну документацію, щодо програмних та програмно-апаратних комплексів захисту інформаційних, інформаційно-комунікаційних систем; виконувати аналіз реалізації прийнятої політики інформаційної і /або кібербезпеки; проектувати та реалізувати системи захисту інформації в інформаційно-комунікаційних системах організації (підприємства) відповідно до вимог нормативних документів системи технічного захисту інформації; вирішувати задачі захисту потоків даних в інформаційних, інформаційно-комунікаційних системах; визначати рівень захищеності інформаційних ресурсів в інформаційно-комунікаційних системах.

Набуття компетентностей:

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

Загальні компетентності:

КЗ 1. Здатність застосовувати знання у практичних ситуаціях.

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

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

Спеціальні (фахові, предметні) компетентності (СК):

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.

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

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

ПРН3. Використовувати результати самостійного пошуку, аналізу та синтезу інформації з різних джерел для ефективного рішення спеціалізованих задач професійної діяльності.

ПРН4. Аналізувати, аргументувати, приймати рішення при розв’язанні складних спеціалізованих задач та практичних проблем у професійній діяльності, які характеризуються комплексністю та неповною визначеністю умов, відповідати за прийняті рішення.

ПРН6. Критично осмислювати основні теорії, принципи, методи і поняття у навчанні та професійній діяльності.

ПРН13. Аналізувати проекти інформаційно-телекомунікаційних систем, базуючись на стандартизованих технологіях та протоколах передачі даних.

ПРН14. Вирішувати завдання захисту програм та інформації, що обробляється в інформаційно-телекомунікаційних системах програмно-апаратними засобами та давати оцінку результативності якості прийнятих рішень.

ПРН17. 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.

ПРН20. Забезпечувати функціонування спеціального програмного забезпечення, щодо захисту інформації від руйнуючих програмних впливів, руйнуючих кодів в інформаційно-телекомунікаційних системах.

ПРН21. 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.

ПРН23. Реалізовувати заходи з протидії отриманню несанкціонованого доступу до інформаційних ресурсів і процесів в інформаційних та інформаційно-телекомунікаційних (автоматизованих) системах.

ПРН29. Здійснювати оцінювання можливості реалізації потенційних загроз інформації, що обробляється в інформаційно-телекомунікаційних системах та ефективності використання комплексів засобів захисту в умовах реалізації загроз різних класів.

ПРН30. Здійснювати оцінювання можливості несанкціонованого доступу до елементів інформаційно-телекомунікаційних систем.

ПРН31. Застосовувати теорії та методи захисту для забезпечення безпеки елементів інформаційно-телекомунікаційних систем.

ПРН50. Забезпечувати) функціонування програмних та програмно-апаратних комплексів виявлення вторгнень різних рівнів та класів (статистичних, сигнатурних, статистично-сигнатурних).

ПРН51. Підтримувати працездатність та забезпечувати конфігурування систем виявлення вторгнень в інформаційно-телекомунікаційних системах.

ПРН52. Використовувати інструментарій для моніторингу процесів в інформаційно-телекомунікаційних 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 інформації в інформаційно-комунікаційних системах» є основним документом, що охоплює всі види навчальної роботи при вивченні курсу студентами та відбиває основні методичні настанови кафедри.

Навчальна програма дисципліни «Безпека інформації в інформаційно-комунікаційних системах» 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 інформації в інформаційно-комунікаційних системах» є курс «Комплексні системи захисту інформації».

Курс «Безпека інформації в інформаційно-комунікаційних системах» є базовим для вивчення наступної дисципліни: «Основи криптоаналізу».

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	всьо-го	у тому числі					всьо-го	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. Основні поняття щодо безпеки інформації в інформаційно-комунікаційних системах.													
Тема 1. Модель взаємодії елементів інформаційно-комунікаційної системи.	1	8	2		2		4						
Тема 2. Побудова систем управління інформаційною безпекою інформаційно-комунікаційних систем.	2	8	2		2		4						
Тема 3. Процедури ідентифікації, автентифікації, авторизації користувачів.	3	8	2		2		4						
Тема 4. Модель загроз безпеці інформації в інформаційно-комунікаційних системах.	4	8	2		2		4						
Тема 5. Модель порушника безпеки інформації в інформаційно-комунікаційних системах.	5	8	2		2		4						
Тема 6. Моделі управління доступом в інформаційно-комунікаційних системах.	6	8	2		2		4						

Тема 7. Моделі безпеки інформації в інформаційно-комунікаційних системах.	7	8	2		2		4						
Разом за змістовим модулем 1		**56**	**14**		**14**		**28**						
Змістовий модуль 2. Забезпечення захисту інформації в інформаційно-комунікаційних системах.													
Тема 1. Методи та засоби забезпечення інформаційної безпеки інформаційно-комунікаційних систем.	9	8	2		2		4						
Тема 2. Фізична безпека інформаційно-комунікаційних систем.	10	8	2		2		4						
Тема 3. Основні підсистеми комплексу засобів захисту в інформаційно-комунікаційних системах.	11	8	2		2		4						
Тема 4. Системи виявлення вторгнень та системи запобігання вторгненням.	12	8	2		2		4						
Тема 5. Реєстрація подій в інформаційно-комунікаційних системах.	13	8	2		2		4						
Тема 6. Моніторинг процесів функціонування інформаційно-комунікаційних систем.	14	8	2		2		4						
Тема 7. Механізми безпеки комп'ютерних мереж.													
Тема 8. Внутрішній аудит безпеки інформації в інформаційно-комунікаційних системах.	15	8	2		2		4						
Разом за змістовим модулем 2		**64**	**16**		**16**		**32**						
Всього годин		**120**	**30**		**30**		**60**						

4. 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	

5. Теми лабораторних занять

№ з/п	Назва теми	Кількість годин
1	Вирішення завдань захисту програм та інформації, що обробляється в інформаційно-комунікаційних системах.	4
2	Дослідження процесів ідентифікації, автентифікації, авторизації та підзвітності та їх застосування в інформаційно-комунікаційних системах..	2
3	Побудова моделі загроз безпеці інформації в інформаційно-комунікаційних системах.	4
4	Побудова моделі порушника безпеки інформації в інформаційно-комунікаційних системах.	2
5	Дослідження моделей управління доступом та їх застосування в інформаційно-комунікаційних системах.	2
6	Застосування моделей безпеки інформації в інформаційно-комунікаційних системах.	2
7	Застосування методів та засобів забезпечення безпеки інформації в інформаційно-комунікаційних системах.	2
8	Розроблення заходів з протидії фізичному несанкціонованому доступу до інформаційних ресурсів і процесів в інформаційно-комунікаційних системах.	2
9	Застосування підсистем комплексу засобів захисту інформації в інформаційно-комунікаційних системах.	4
10	Розроблення правил адміністрування інформаційно-комунікаційної системи	4
11	Вирішення завдань з організації проведення внутрішнього аудиту безпеки інформації в інформаційно-комунікаційних системах.	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	Завдань захисту програм та інформації, що обробляється в інформаційно-комунікаційних системах.	6
2	Моделі загроз безпеці інформації в інформаційно-комунікаційних системах.	6
3	Системи виявлення вторгнень та системи запобігання вторгненням.	6
4	Моделі управління доступом та їх застосування в інформаційно-комунікаційних системах.	6
5	Моделі безпеки інформації в інформаційно-комунікаційних системах.	6
6	Методи та засоби забезпечення безпеки інформації в інформаційно-комунікаційних системах.	6
7	Заходи з протидії фізичному несанкціонованому доступу до інформаційних ресурсів і процесів в інформаційно-комунікаційних системах.	6
8	Реєстрація подій в інформаційно-комунікаційних системах.	6
9	Внутрішній аудит безпеки інформації в інформаційно-комунікаційних системах.	6
10	Завдання з організації проведення внутрішнього аудиту безпеки інформації в інформаційно-комунікаційних системах.	6
	Всього	60

Контрольні питання, комплекти тестів для визначення рівня засвоєння знань студентами

1.1. Питання для перевірки знань студентів:

1. Принципи створення систем інформаційної безпеки в ІКС.
2. Основні підсистеми системи інформаційної безпеки ІКС.
3. Сутність і функції адміністратора безпеки.
4. Сутність і функції системного адміністратора.
5. Повноваження адміністратора безпеки щодо доступу до інформаційних ресурсів.

6. Повноваження системного адміністратора щодо доступу до інформаційних ресурсів.
7. Повноваження користувачів щодо доступу до інформаційних ресурсів.
8. Повноваження адміністратора безпеки щодо управління засобами захисту інформації.
9. Повноваження системного адміністратора щодо управління засобами захисту інформації.
10. Повноваження користувачів щодо управління засобами захисту інформації.
11. Можливості адміністратора безпеки, що надаються йому засобами ІКС.
12. Можливості системного адміністратора, що надаються йому засобами ІКС.
13. Можливості користувачів, що надаються їм засобами ІКС.
14. Сутність внутрішнього порушника інформаційної безпеки.
15. Сутність зовнішнього порушника інформаційної безпеки.
16. Завдання, що покладаються на фізичні засоби захисту.
17. Механізми захисту периметру.
18. Сутність витоку інформації.
19. Сутність моделі кінцевих автоматів.
20. Сутність моделі Bell-LaPadula.
21. Сутність моделі Biba.
22. Сутність моделі Clark-Wilson.
23. Причини виникнення прихованих каналів для несанкціонованої передачі даних.
24. Типи прихованих каналів для несанкціонованої передачі даних.
25. Ідентифікація, автентифікація, авторизація.
26. Сутність двофакторної автентифікації.
27. Типи моделей управління доступом.
28. Класифікація технік управління доступом.
29. Системи виявлення вторгнень.
30. Системи запобігання вторгненням.
31. Групи подій і дій, які необхідно реєструвати і вносити в журнал.
32. Типи інструментів аналізу журналів реєстрації подій.
33. Сутність ідентифікації інформаційних активів.
34. Методи ідентифікації ризику.
35. Сутність аудиту інформаційної безпеки.
36. Мета проведення аудиту інформаційної безпеки.

1.2. Приклади тестів з дисципліни:

1. Отримує доступ до всіх серверів, робочих станцій та комутаційного обладнання на рівні адміністрування …:

А) адміністратор безпеки;

В) спеціально уповноважений центральний орган виконавчої влади з питань організації спеціального зв'язку та захисту інформації і підпорядковані йому регіональні органи;

С) системний адміністратор.

2. Контрольована зона - це ...

А) простір навколо технічного засобу захисту, в межах якого не допускається розташування інших технічних засобів, через які може витікати таємна інформація;

В) територія об’єкту, на якому виключена можливість безконтрольного перебування осіб та транспортних засобів, що не мають постійних або разових перепусток;

С) мінімально допустима зона навколо технічного засобу захисту, на границі та за межами якої напруженості електричного та магнітного полів небезпечного сигналу відносно шумових завад не перевищують нормованого значення.

3. Здійснює управління конфігураціями та системними налаштуваннями серверів, робочих станцій та комутаційним обладнанням:

А) користувач;

В) приймання робіт з оцінкою їх відповідності вимогам ТЗ;

С) системний адміністратор.

2. Методи навчання

Виконання лабораторних робіт з використанням персонального комп’ютера; 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

Основні:

1. НД ТЗІ 3.7-003 -2005 «Порядок проведення робіт із створення комплексної системи захисту інформації в інформаційно-телекомунікаційній системі» // Департамент спеціальних телекомунікаційних систем та захисту інформації Служби безпеки України. Київ. 2005. – С. 22.
2. Закон України «Про захист інформації в автоматизованих системах» // Відомості Верховної Ради України, 1994. - № 31. – С. 286.
3. Кормич Б.А. Інформаційна безпека: організаційно-правові основи. / Б.А. Кормич. − К., Принт. 2004. -169 с.
4. Методи та засоби захисту інформації [Навчальний посібник] / В.А. Лахно, Є.В. Василіу, В.М. Гладких, В.М. Домрачев, Н.М. Сивкова. – К. : ЦП «Компринт» О.В., 2020. – 444 с.
5. Кузнецов О. О. Захист інформації в інформаційних системах. Методи традиційної криптографії / О.О. Кузнецов, С.П. Євсеєв, О.Г. Король. – Х.: Вид. ХНЕУ, 2010. – 316 с.
6. Браіловський М.М. Захист інформації у банківській діяльності / М.М. Браіловський, Г.П. Лазарєв, В.О. Хорошко. – К.: ТОВ “ПоліграфКонсалтинг”, 2010. – 216 с.
7. Проєктування комплексних систем захисту інформації. Підручник / В. О. Хорошко, І. М. Павлов, Ю. Я. Бобало, В. Б. Дудикевич, І. Р. Опірський, Л. Т. Пархуць. Львів : Видавництво Львівської політехніки, 2020. 320 с.
8. Технології захисту інформації : навчальний посібник / С. Е. Остапов, С. П. Євсеєв, О. Г. Король. – Х. : Вид. ХНЕУ, 2013. – 476 с. (Укр. мов.).
9. Основи інформаційної безпеки / С. В. Кавун, О. А. Смірнов, В. Ф. Столбов – Кіровоград : Вид. КНТУ, 2012. – 414 с.

Допоміжні

1. Yevseiev, S., Ponomarenko, V., Laptiev, O., Milov, O., Korol, O., Milevskyi, S., ... & Florov, S. (2021). Synergy of building cybersecurity systems.

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