НАЦІОНАЛЬНИЙ УНІВЕРСИТЕТ БІОРЕСУРСІВ І ПРИРОДОКОРИСТУВАННЯ УКРАЇНИ

Кафедра комп'ютерних систем, мереж та кібербезпеки

"ЗАТВЕРДЖУЮ"
Декан факультету інформаційних технологій

проф. О.Г. Глазунова
_____ 2022 р.

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 «Комп'ютерні системи і мережі»
_____ (Гусєв Б.С.)

«КОМПЛЕКСНІ СИСТЕМИ САНКЦІОНОВАНОГО ДОСТУПУ ДО ІНФОРМАЦІЇ»

Спеціальність	123 «Комп'ютерна інженерія»
Освітня програма	«Комп'ютерні системи і мережі»
Факультет	інформаційних технологій
Розробник:	Лахно В.А., д.т.н., професор

Київ – 2022

1. Опис навчальної дисципліни
«Комплексні системи санкціонованого доступу до інформації»

Галузь знань, спеціальність, освітня програма, освітній ступінь		
Освітній ступінь	Магістр	
Галузь знань	12 – Інформаційні технології	
Спеціальність	123 – Комп'ютерна інженерія	
Освітня програма	«Комп'ютерні системи і мережі»	
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	1	
Семестр	2	
Лекційні заняття, год.	20	
Практичні, семінарські заняття	-	
Лабораторні заняття, год.	30	
Самостійна робота, год.	70	
Індивідуальні завдання	-	
Кількість тижневих аудиторних годин для денної форми навчання	10 (5 тижнів)	

2. Мета, завдання та компетентності навчальної дисципліни

Навчальна дисципліна передбачає надання майбутньому спеціалісту чіткого розуміння про моделі, методи та апаратно-програмні засоби для вирішення задач побудови комплексних систем санкціонованого доступу до інформації об'єктів інформатизації.

Завдання навчальної дисципліни: ознайомленні студентів із головними питаннями курсу; викладенні студентам у відповідності з програмою та робочим планом основних питань курсу; формуванні у студентів цілісної системи теоретичних знань з курсу «Комплексні системи санкціонованого доступу до інформації».

В результаті вивчення навчальної дисципліни студент повинен

знати:

– основні процеси що вимагаються при впровадженні КСЗІ;

– класифікацію та характеристики апаратних засобів для ефективного впровадження КСЗІ;

– основні чинники, що визначають надійність і ефективність КСЗІ;

– понятійно-термінологічний апарат в області аналізу та впровадження КСЗІ.

вміти:

– визначати тип каналів витоку;

– аналізувати ефективність обраного засобу технічного захисту;

– виявляти особливості КСЗІ для різних типів задач;

– обґрунтовувати вибір технічних і організаційних засобів для ефективного впровадження КСЗІ;

– визначати ресурси, необхідні для забезпечення надійності функціонування КСЗІ з врахуванням факторів помилки у роботі користувачів.

Набуття компетентностей:

Відповідно до освітньої програми підготовки фахівців за спеціальністю 123 «Комп'ютерна інженерія» навчальна дисципліна забезпечує формування загальних і фахових компетентностей:

Загальні компетентності:

ЗК5. Здатність генерувати нові ідеї (креативність).

ЗК6. Здатність виявляти, ставити та вирішувати проблеми.

ЗК7. Здатність приймати обґрунтовані рішення.

Спеціальні (фахові, предметні) компетентності (СК):

СК3. Здатність проектувати комп'ютерні системи та мережі з урахуванням цілей, обмежень, технічних, економічних та правових аспектів.

СК5. Здатність будувати архітектуру та створювати системне і прикладне програмне забезпечення комп'ютерних систем та мереж.

СК6. Здатність використовувати та впроваджувати нові технології, включаючи технології розумних, мобільних, зелених і безпечних обчислень, брати участь в модернізації та реконструкції комп'ютерних систем та мереж, різноманітних вбудованих і розподілених додатків, зокрема з метою підвищення їх ефективності.

СК8. Здатність забезпечувати якість продуктів і сервісів інформаційних технологій на протязі їх життєвого циклу.

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

РН 4. Застосовувати спеціалізовані концептуальні знання, що включають сучасні наукові здобутки у сфері комп'ютерної інженерії, необхідні для професійної діяльності, оригінального мислення та проведення досліджень, критичного осмислення проблем інформаційних технологій та на межі галузей знань

РН 5. Розробляти і реалізовувати проекти у сфері комп'ютерної інженерії та дотичні до неї міждисциплінарні проєкти з урахуванням інженерних, соціальних, економічних, правових та інших аспектів.

РН 6. Аналізувати проблематику, ідентифікувати та формулювати конкретні проблеми, що потребують вирішення, обирати ефективні методи їх вирішення.

РН 7. Вирішувати задачі аналізу та синтезу комп'ютерних систем та мереж.

РН 8. Застосовувати знання технічних характеристик, конструктивних особливостей, призначення і правил експлуатації програмно-технічних засобів комп'ютерних систем та мереж для вирішення складних задач комп'ютерної інженерії та дотичних проблем.

РН 9. Розробляти програмне забезпечення для вбудованих і розподілених застосувань, мобільних і гібридних систем.

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 магістра за спеціальністю «Комп'ютерна інженерія».

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

Навчальна програма дисципліни розроблена на підставі наступних документів:

- освітня програма підготовки магістрів за спеціальністю 123 «Комп'ютерна інженерія»;
- навчальний план підготовки магістрів за спеціальністю 123 «Комп'ютерна інженерія».

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 «Комплексні системи санкціонованого доступу до інформації» є курси «Комп'ютерна електроніка», «Комп'ютерна схемотехніка», «Захист інформації в комп'ютерних системах» ОПП першого (бакалаврського) рівня вищої освіти.

3. Програма та структура навчальної дисципліни

– повного терміну денної (заочної) форми навчання;

Назви змістових модулів і тем	Кількість годин												
	денна форма							Заочна форма					
	тижні	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. Завдання та методологічні основи КСЗІ.													
Тема 1. Методологічні основи комплексної системи захисту інформації.	1	9	2		0		7						
Тема 2. Визначення складу інформації, що захищається на підприємстві.	1	13	2		4		7						
Тема 3. Джерела, способи і результати дестабілізуючого впливу на інформацію.	2	13	2		4		7						
Тема 4. Канали і методи несанкціонованого доступу до інформації.	2	13	2		4		7						
Тема 5. Технічні засоби комплексних системи санкціонованого доступу до інформації.	3	13	2		4		7						
Разом за змістовим модулем 1		**61**	**10**		**16**		**35**						
Змістовий модуль 2. Моделювання, технологічна побудова, апаратні компоненти КСЗІ.													
Тема 6. Моделювання процесів комплексної системи захисту інформації.	3	11	2		2		7						
Тема 7. Технологічна побудова комплексної системи захисту інформації.	4	9	2		0		7						
Тема 8. Управління комплексною системою захисту інформації.	4	13	2		4		7						
Тема 9. Планування діяльності комплексної системи захисту інформації на підприємстві.	5	13	2		4		7						
Тема 10. Управління комплексною системою захисту інформації в умовах таргетованих кібератак на підприємство.	5	13	2		4		7						
Разом за змістовим модулем 2		**59**	**10**		**14**		**35**						
Всього годин		**120**	**20**		**30**		**70**						

4. Теми лабораторних занять

№ з/п	Назва теми	Кількість годин
1.	Дослідження системи аналізу ризиків та перевірки політики інформаційної безпеки підприємства.	2
2.	Дослідження захищеності бездротових мереж передачі даних підприємства.	4

3.	Дослідження і адміністрування засобів забезпечення інформаційної безпеки Web-сервера Microsoft IIS Server.	4
4.	Дослідження і адміністрування коштів забезпечення інформаційної безпеки Microsoft ISA Security Server.	4
5.	Встановлення та налаштування брандмауера ISA. Побудова VPN-мережі на базі ISA.	4
6.	Оцінка загроз в інформаційних системах підприємств АПК.	4
7.	«Протокол випробувань комплексних систем захисту інформації». Супроводження КСЗІ.	4
8.	Дослідження та розгортання мережевої інфраструктури Microsoft Windows Exchange Server.	4
	Разом за семестр	**30**
	Разом	**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.

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

5.1. Питання для перевірки знань студентів:

1. Надайте визначення інформаційної безпеки.
2. Надайте визначення загрози інформаційній безпеці.
3. Як поділяється інформація за режимом доступу до неї?
4. Які грифи таємності можуть надаватися інформації та який їх терміни дії?
5. Яка інформація не відноситься до державної таємниці?
6. Надайте визначення ТЗІ.
7. Які основні заходи з організації створення КСЗІ?
8. Який порядок проведення обстеження на об’єкті інформаційної діяльності?
9. Які розділи і підрозділи входять до складу технічного завдання на створення КСЗІ?
10. Які вимоги та функції висуваються до засобів антивірусного захисту?
11. Яка мета та порядок проведення обстеження та атестації виробництва?
12. Які заходи організовує та виконує виконавець робіт зі створення КСЗІ?
13. Які розділи містить технічне завдання на створення КСЗІ?
14. Який порядок розроблення та оформлення технічного завдання на створення КСЗІ?
15. Яка мета та порядок контролю за станом технічного захисту інформації?

5.2. Приклади тестових питань з дисципліни:

1. Сучасні методики та програмні засоби побудови моделей загроз для інформації та порушників в ІКС?
2. Опис сучасних загроз для інформації та нормального функціонування ІКС?
3. Сучасні методики та програмні засоби формування ФПЗ інформації від НСД в ІКС?
4. Сучасні методики та програмні засоби оцінки стану захищеності інформації Web-сайту від НСД?

5. Сучасні методики та програмні засоби оцінки надійності та ефективності КСЗІ в ІКС?

6. Опис стану оформлення та провадження господарської діяльності у галузі ТЗІ в Україні?

7. Опис стану оформлення та провадження господарської діяльності у галузі КЗІ в Україні (крім ЕЦП)?

6. Методи навчання

Виконання лабораторних робіт з використанням ПЗ Microsoft IIS Server, Microsoft ISA Security Server, брандмауер ISA, Windows Exchange Server; виконання індивідуальних навчально-дослідних завдань.

7. 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.

8. 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 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): $R_{дис}=R_{НР}+R_{АТ}$.

9. Методичне забезпечення

1. Конспект лекцій з курсу "Комплексні системи санкціонованого доступу до інформації". - Київ, НУБіП, 2020.

10. Рекомендована література

Базова:

1. Закон України «Про захист інформації в інформаційно-телекомунікаційних системах» [Електронний ресурс] / База законодавства України // № 80/94-ВР – Режим доступу: http://zakon4.rada.gov.ua/laws/show/80

2. Комплекс засобів захисту від НСД в АС класу 1 «Рубіж-РСО» версія 2 [Електронний ресурс] / ТОВ «Технічний захист інформації» // 2013 - Режим доступу: http://tzi.com.ua/rubzh-rso-versya20.html

3. Комплексні системи захисту інформації: проектування, впровадження, супровід. Збірник лекцій [Електронний ресурс] / Гребенніко В.В. // 2015 - Режим доступу: http://www.cryptohistory.ru/for students/ 03-KSZI

4. Операційна система «OpenBSD, шифр BBOS» [Електронний ресурс] / Кампанія «ATMNIS» // 2012 - Режим доступу: http://www.atmnis.com/files/user files/BBOS overview.pdf

5. Порядок проведення робіт із створення комплексної системи захисту інформації в інформаційно-телекомунікаційній системі. НД ТЗІ 3.7-003-05 [Електронний ресурс] / Нормативна база Держспецзв'язку // 2015 - Режим доступу:http://www.dstszi.gov.ua/dstszi/control/uk/publish/article?art id=46074

6. Стратегія національної безпеки України (затверджена Указом Президента України від 26 травня 2015 року № 287/2015)

7. Закон України "Про національну безпеку (2018)

8. Стратегія кібербезпеки України" (Введено в дію Указом Президента України від 15 березня 2016 року №96/2016)

9. НД ТЗІ 1.6-004-2013 Захист інформації на об'єктах інформаційної діяльності. Положення про категоріювання об'єктів, де циркулює інформація з обмеженим доступом, що становить державну таємницю.

10. Information Security Handbook for Network Beginners. National Center of Incident Readiness and Strategy for Cybersecurity (NISC) ver. 2.11e

11. Захист інформації в автоматизованих системах управління : навчальний посібник / Уклад. І. А. Пількевич, Н. М. Лобанчикова, К. В. Молодецька. – Житомир : Вид-во ЖДУ ім. І. Франка, 2015. – 226 с.

Допоміжна

12. Логінова Н. І. правовий захист інформації : навчальний посібник / Н. І. Логінова, Р. Р. Дробожур. – Одеса : Фенікс, 2015. – 264 с.

13. Бурячок В. Л. Інформаційний та кіберпростори: проблеми безпеки, методи та засоби боротьби : посібник / [В. Л. Бурячок, С. В. Толюпа, В. В. Семко та ін.]. – К. : ДУТ-КНУ, 2016. – 178 с.

Інформаційні ресурси

1. https://cip.gov.ua/ua/statics/licenzuvannya