Київський університет імені Бориса Грінченка

Факультет інформаційних технологій та математики

Кафедра інформаційної та кібернетичної безпеки

імені професора Володимира Бурячка

«ЗАТВЕРДЖУЮ»
Проректор з науково-методичної
та навчальної роботи
_____ Олексій ЖИЛЬЦОВ
«___»_____ 2023

РОБОЧА ПРОГРАМА НАВЧАЛЬНОЇ ДИСЦИПЛІНИ «ПРИКЛАДНІ АСПЕКТИ ПОБУДОВИ КТЗІ»

для студентів

спеціальності 125 Кібербезпека

освітнього рівня першого (бакалаврського)
освітньої програми 125.00.01 Безпека інформаційних і комунікаційних систем

2023 – 2024 навчальний рік

Розробник:
Козачок Валерій Анатолійович, кандидат технічних наук, доцент, доцент кафедри інформаційної та кібернетичної безпеки імені професора Володимира Бурячка Факультету інформаційних технологій та математики Київського університету імені Бориса Грінченка.

Викладач:
Козачок Валерій Анатолійович, кандидат технічних наук, доцент, доцент кафедри інформаційної та кібернетичної безпеки імені професора Володимира Бурячка Факультету інформаційних технологій та математики Київського університету імені Бориса Грінченка.

Робочу програму розглянуто і затверджено на засіданні кафедри інформаційної та кібернетичної безпеки імені професора Володимира Бурячка
Протокол від 01.09.2022 р. № 12

Завідувач кафедри _____ (підпис) Павло СКЛАДАННИЙ

Робочу програму погоджено з гарантом освітньої програми (керівником освітньої програми 125.00.01 Безпека інформаційних і комунікаційних систем)

___.___. 2022 р.
Керівник освітньої програми _____ (підпис) Артем ПЛАТОНЕНКО

Робочу програму перевірено
___.___. 2022 р.
Заступник декана _____ (підпис) Євген ІВАНІЧЕНКО

Пролонговано:
на 2023/2024 н.р. _____ (підпис) _____ (ПІБ), «23» 08 2023 р., протокол № 8
на 20__/20__ н.р. _____ (підпис) (_____ (ПІБ)), «____»____ 20___ р., протокол № ___
на 20__/20__ н.р. _____ (підпис) (_____ (ПІБ)), «____»____ 20___ р., протокол № ___
на 20__/20__ н.р. _____ (підпис) (_____ (ПІБ)), «____»____ 20___ р., протокол № ___

1. Опис навчальної дисципліни

Найменування показників	Характеристика дисципліни за формами навчання	
	денна	заочна
Вид дисципліни	вибіркова	
Мова викладання, навчання та оцінювання	українська	
Загальний обсяг кредитів / годин	5 / 150	
Курс	2	
Семестр	4	
Кількість змістових модулів з розподілом:	2	
Обсяг кредитів	5	
Обсяг годин, в тому числі:	150	
Аудиторні	56	
Модульний контроль	8	
Семестровий контроль	30	
Самостійна робота	56	
Форма семестрового контролю	екзамен	

2. Мета та завдання навчальної дисципліни

Робоча навчальна програма з курсу «Прикладні аспекти побудови КТЗІ» є нормативним документом Київського університету імені Бориса Грінченка, який розроблено кафедрою інформаційної та кібернетичної безпеки імені професора Володимира Бурячка на основі освітньо-професійної програми підготовки здобувачів першого (бакалаврського) рівня відповідно до навчальних планів спеціальності 125 Кібербезпека.

Робочу навчальну програму укладено згідно з вимогами Європейської кредитної трансферно-накопичувальної системи (ЄКТС) організації навчання.

Програма визначає обсяги знань, якими повинен опанувати здобувач першого (бакалаврського) рівня відповідно до вимог освітньо-кваліфікаційної характеристики, алгоритму вивчення навчального матеріалу дисципліни «Прикладні аспекти побудови КТЗІ» та необхідне методичне забезпечення, складові і технологію оцінювання навчальних досягнень студентів.

Навчальна дисципліна «Прикладні аспекти побудови КТЗІ» складається з двох змістових модулів: Основи створення КТЗІ, Основні етапи побудови КТЗІ на ОІД. Обсяг дисципліни – 150 год (5 кредитів).

Метою викладання навчальної дисципліни «Прикладні аспекти побудови КТЗІ» є отримання компетентностей зі створення комплексу технічного захисту інформації на об’єктах інформаційної діяльності.

Завдання:

- надання студентам теоретичних знань про засоби і методи організаційного захисту інформації;
- формування у студентів категоріальних понять з принципів побудови КТЗІ;
- формування у студентів уміння аналізу ефективності КТЗІ;
- стимулювання студентів до активної аналітико-пошукової роботи, що спрямована на визначення ефективних шляхів застосування систем технічного захисту інформації.

У результаті вивчення навчальної дисципліни формуються

загальні компетентності:

КЗ-2: Здатність до здобування нових знань, накопичення наукових та педагогічних вмінь і навичок та їх застосування в практичних ситуаціях

КЗ-3: Здатність до виявлення, генерування, дослідження та вирішення проблем за професійним спрямуванням.

фахові компетентності:

КФ-7: Здатність впроваджувати та забезпечувати функціонування комплексних систем захисту інформації (комплекси нормативно-правових, організаційних та технічних засобів і методів, процедур, практичних прийомів та ін.)

3. Результати навчання за дисципліною

При вивченні курсу «Прикладні аспекти побудови КТЗІ» студенти повинні

знати:

- історію та особливості розвитку систем технічного захисту інформації;
- основні процеси що вимагаються при впровадженні КТЗІ;
- класифікацію та характеристики апаратних засобів для ефективного впровадження КТЗІ;
- основні чинники, що визначають надійність і ефективність КТЗІ;
- понятійно-термінологічний апарат в області аналізу та впровадження КТЗІ;

уміти:

- визначати тип каналів витоку;
- аналізувати ефективність обраного засобу технічного захисту,
- виявляти особливості КТЗІ для різних типів задач;
- обґрунтовувати вибір технічних засобів і організаційних заходів для ефективного впровадження КТЗІ;
- визначати ресурси, необхідні для забезпечення надійності функціонування КТЗІ з врахуванням факторів помилки у роботі користувачів.

та досягнути наступні ***програмні результати***:

ПРз-5	- обирати основні методи та засоби захисту інформації відповідно до вимог сучасних стандартів інформаційної і кібербезпеки, та критеріїв безпеки інформаційних технологій, застосовуючи системний підхід та знання основ теорії захисту інформації; - вирішувати задачі управління процедурами ідентифікації, автентифікації, авторизації, користувачів і процесів в інформаційних та інформаційно-телекомунікаційних (автоматизованих) системах - проектувати та реалізувати комплексні системи захисту інформації в АС організації (підприємства) відповідно до вимог нормативних документів системи технічного захисту інформації; - вирішувати задачі захисту потоків даних в інформаційних, інформаційно-телекомунікаційних (автоматизованих) системах; - визначати рівень захищеності інформаційних ресурсів в інформаційних та інформаційно-телекомунікаційних (автоматизованих) системах; - використовувати інструментальні засоби оцінювання можливості реалізації потенційних загроз інформації, що обробляється в інформаційно-телекомунікаційних (автоматизованих) системах;
ПРз-7	- вирішувати задачі супроводу та впровадження комплексних систем захисту інформації, а також протидії несанкціонованому доступу до ресурсів і процесів в інформаційних та інформаційно-телекомунікаційних (автоматизованих) системах; - здійснювати оцінку рівня захищеності інформації що обробляється в ІТС використовувати інструментальні засоби оцінювання наявності потенційних вразливостей; - вирішувати задачі управління комплексною системою захисту інформації в інформаційних та інформаційно-телекомунікаційних (автоматизованих); - вирішувати задачі експертизи, випробування КСЗІ;

4. Структура навчальної дисципліни

Тематичний план для денної форми навчання

Назва змістових модулів, тем	Усього	Розподіл годин між видами робіт				
		Аудиторна:				Самостійна
		Лекції	Семінари	Практичні	Лабораторні	
Змістовий модуль 1. Основи створення КТЗІ						
Тема 1. Введення в дисципліну. Основні терміни та визначення. Нормативно-правова база створення КТЗІ.	6	2				4
Тема 2. Класифікація технічних каналів витоку інформації. Методи та засоби несанкціонованого отримання інформації по технічним каналам.	26	2			12	12
Тема 3. Засоби та заходи захисту інформації від витоку по технічним каналам.	26	2			12	12
Модульний контроль	4					
Разом	62	6			24	28
Змістовий модуль 2. Основні етапи побудови КТЗІ на ОІД						
Тема 4. Порядок створення комплексу технічного захисту інформації на об’єкті інформаційної діяльності.	46	4		18		24
Тема 5. Випробування та атестація КТЗІ.	8	2		2		4
Модульний контроль	4					
Разом	58	6		20		28
Семестровий контроль	30					
Усього	150	12		20	24	56

5. Програма навчальної дисципліни

Змістовий модуль 1. Основні поняття щодо побудови КТЗІ.

Основні питання:

- Нормативно-правова база створення КТЗІ.
- Класифікація технічних каналів витоку інформації.
- Методи та засоби несанкціонованого отримання інформації по технічним каналам.
- Засоби та заходи захисту інформації від витоку по технічним каналам.

Змістовий модуль 2. Порядок створення КТЗІ на ОІД

Основні питання:

- Порядок створення КТЗІ на ОІД.
- Випробування та атестація КТЗІ.

6. Контроль навчальних досягнень

Навчальні досягнення студентів з дисципліни оцінюються за модульно-рейтинговою системою, в основу якої покладено принцип пооперaційної звітності, обов'язковості модульного контролю, накопичувальної системи оцінювання рівня знань, умінь та навичок, розширення кількості підсумкових балів до 100.

Оцінка за кожний змістовий модуль включає бали за поточну роботу студента на практичних заняттях та семінарах, за виконання індивідуальних завдань, за модульну контрольну роботу. Виконання модульних контрольних робіт здійснюється в електронному вигляді. Модульний контроль знань студентів здійснюється після завершення вивчення навчального матеріалу змістового модуля.

У процесі оцінювання навчальних досягнень студентів застосовуються такі методи:

- *методи усного контролю*: індивідуальне опитування, фронтальне опитування, співбесіда, екзамен;
- *комп'ютерного контролю:* тестові програми;
- *методи самоконтролю:* уміння самостійно оцінювати свої знання, самоаналіз.

Кількість балів за роботу з теоретичним матеріалом, на практичних заняттях, під час виконання самостійної роботи залежить від дотримання таких вимог:

- систематичність відвідування занять;
- своєчасність виконання навчальних та індивідуальних завдань;
- повний обсяг їх виконання;
- якість виконання навчальних та індивідуальних завдань;
- самостійність виконання;
- творчий підхід у виконанні завдань;
- ініціативність у навчальній діяльності;
- виконання тестових завдань.

Контроль успішності студентів з урахуванням поточного і підсумкового оцінювання здійснюється відповідно до навчально-методичної карти дисципліни, де зазначено види контролю і кількість балів за видами. Систему рейтингових балів для різних видів контролю та порядок їх переведення у національну (4-бальну) та європейську (ECTS) шкалу подано нижче у таблицях.

Розрахунок рейтингових балів за видами поточного (модульного) контролю

Вид діяльності студента	Максимальна к-сть балів за одиницю	Модуль 1		Модуль 2	
		кількість одиниць	максимальна кількість балів	кількість одиниць	максимальна кількість балів
Відвідування лекцій	1	3	3	3	3
Відвідування практичних занять	1	-	-	10	10
Відвідування лабораторних робіт	1	12	12	-	-
Робота на практичному занятті	10	-	-	10	100
Робота на лабораторному занятті	10	12	120	-	-
Виконання завдань для самостійної роботи	5	1	5	1	5
Виконання модульної роботи	25	1	25	1	25
Виконання ІНДЗ	30				
	Разом	-	165	-	143
Максимальна кількість балів: 308					
Розрахунок коефіцієнта: 308/100=3,08					

Завдання для самостійної роботи та критерії її оцінювання

Самостійна робота є видом поза аудиторної індивідуальної діяльності студента, результати якої використовуються у процесі вивчення програмового матеріалу навчальної дисципліни та містить результати дослідницького пошуку, відображає певний рівень його навчальної компетентності.

Перелік тем та оцінювання самостійної роботи студента

№ з/п	Назва теми	Кількість годин	Бали
Змістовий модуль 1. Основи створення КТЗІ		**28**	**5**
1	Основні терміни та визначення. Нормативно-правова база створення КТЗІ.	4	1
2	Класифікація технічних каналів витоку інформації. Методи та засоби несанкціонованого отримання інформації по технічним каналам.	12	2
3	Засоби та заходи захисту інформації від витоку по технічним каналам.	12	2
Змістовий модуль 2. Основні етапи побудови КТЗІ на ОІД		**28**	**5**
4	Порядок створення КТЗІ на ОІД.	24	4
5	Випробування та атестація КТЗІ.	4	1
	Разом	56	10

Критерії оцінювання самостійної роботи студента

№ п/п	Критерії оцінювання роботи	Максимальна кількість балів за кожним критерієм
1	Критичний аналіз суті та змісту першоджерел. Виклад фактів, ідей, результатів досліджень в логічній послідовності. Аналіз сучасного стану дослідження проблеми, розгляд тенденцій подальшого розвитку даного питання.	2 бали
2	Доказовість висновків, обгрунтованість власної позиції, пропозиції щодо розв’язання проблеми, визначення перспектив дослідження	2 бали
3	Дотримання вимог щодо технічного оформлення	1 бал
	Разом	5 балів

Форми проведення модульного контролю та критерії оцінювання

Модульний контроль здійснюється відповідно до навчально-методичної карти дисципліни та перевіряє рівень досягнення результатів навчання студентів. Форма проведення – комп’ютерний тест, що складається 15 запитань закритої та відкритої форм.

Модульна контрольна робота оцінюється у 25 балів.

Форми проведення семестрового контролю та критерії оцінювання

Семестрове (підсумкове) оцінювання здійснюється у формі екзамену, умовою допуску до якого є отриманням студентом 35 балів (з врахуванням коефіцієнту) за результатами поточного контролю.

Екзамен проводиться в університетській аудиторії у комбінованій формі із використанням персональних комп’ютерів, якщо ситуація дозволяє проведення освітнього процесу у традиційній формі. Якщо освітній процес проходить дистанційно, то екзамен проводиться в режимі відеоконференції засобами Google Meet.

Екзамен оцінюється у 40 балів за розподілом: 20 балів – письмова відповідь; 20 балів – захист проекту згідно обраної теми. Студент дає письмову відповіді на три теоретичні питання. Перевірка у ручному режимі. При дистанційному проведенні екзамену студент повинен розмістити відповідь на білет окремим файлом в системі Moodle; ці завдання передбачають ручну перевірку

викладачем.

Орієнтовний перелік питань для семестрового контролю

1. Загальна класифікація видів інформації, що може бути об’єктом злочинних посягань.
2. Надати визначення терміну «Технічний канал витоку інформації».
3. Класифікація технічних каналів витоку інформації.
4. Що собою представляють візуально-оптичні канали витоку інформації?
5. Класифікація способів прихованого відео спостереження та зйомки.
6. Надати визначення терміну «Захист інформації від витоку по візуально-оптичному каналу».
7. Рекомендації щодо захисту інформації від витоку по візуально-оптичному каналу.
8. Комбіновані методи та засоби зняття акустичної інформації.
9. Методи та засоби зняття акустичної інформації з будівельних конструкцій.
10. Методи та засоби зняття акустичної інформації з засобів та ліній зв’язку.
11. Види радіомікрофонів для зняття акустичної інформації.
12. Методи та засоби захисту інформації від витоку акустичними каналами.
13. Пасивні методи захисту акустичної (мовної) інформації.
14. Активні методи захисту акустичної (мовної) інформації.
15. Основні вимоги та рекомендації щодо захисту мовної інформації, яка циркулює в приміщенні.
16. Класифікація електромагнітних каналів витоку інформації.
17. Методи та засоби зняття електромагнітної та електронної інформації.
18. Пасивні методи захисту електромагнітної інформації.
19. Активні методи захисту електромагнітної інформації.
20. Захист інформації в телекомунікаційних системах за рахунок структурної скритності сигналів.
21. Захист інформації в телекомунікаційних системах за рахунок інформаційної скритності.
22. Що собою представляють матеріально-речові канали витоку інформації?
23. Методи та засоби захисту інформації від витоку матеріально-речовими каналами.
24. В яких випадках передбачається створення комплексу ТЗІ на ОІД?
25. Основні етапи створення комплексу ТЗІ на ОІД.
26. Які об’єкти підлягають обов’язковому категоріюванню?
27. Які види категоріювання ОІД ви знаєте?
28. Порядок категоріювання об’єктів.
29. Мета обстеження ОІД.
30. Що аналізується під час проведення обстеження на ОІД?
31. Послідовність проведення робіт з обстеження на ОІД.
32. Зміст технічного завдання на виконання робіт зі створення комплексу технічного захисту інформації на ОІД.
33. Склад «Програми і методики випробувань» КТЗІ.
34. Форма та зміст Акту атестацій комплексу ТЗІ.
35. Структура паспорта на комплекс ТЗІ.

Шкала відповідності оцінок

Рейтингова оцінка	Сума балів за всі види навчальної діяльності	Значення оцінки
A	90-100	Відмінно — відмінний рівень знань (умінь) в межах обов'язкового матеріалу з, можливими, незначними недоліками
B	82-89	Дуже добре - достатньо високий рівень знань (умінь) в межах обов'язкового матеріалу без суттєвих (грубих) помилок
C	75-81	Добре - в цілому добрий рівень знань (умінь) з незначною кількістю помилок
D	69-74	Задовільно - посередній рівень знань (умінь) із значною кількістю недоліків, достатній для подальшого навчання або професійної діяльності
E	60-68	Достатньо - мінімально можливий допустимий рівень знань (умінь)
FX	35-59	Незадовільно з можливістю повторного складання - незадовільний рівень знань, з можливістю повторного перескладання за умови належного самостійного доопрацювання
F	1-34	Незадовільно з обов'язковим повторним вивченням курсу - досить низький рівень знань (умінь), що вимагає повторного вивчення дисципліни

7. Навчально-методична картка дисципліни

Разом: 120 год., лекції – 12 год., практичні заняття – 20 год., лабораторні – 24 год., модульний контроль – 8 год., семестровий контроль – 30 год, самостійна робота – 56 год.

Модулі (назви, бали)	**Змістовий модуль 1. Основні етапи впровадження КТЗІ (165 балів)**			**Змістовий модуль 2. Організаційні заходи для ефективного функціонування КТЗІ (143 бали)**	
Лекції (теми, бали)	№ 1. Введення в дисципліну. Основні терміни та визначення. Нормативно-правова база створення КТЗІ. (1 бал)	№ 2. Класифікація технічних каналів витоку інформації. Методи та засоби несанкціонованого отримання інформації по технічним каналам. (1 бал)	№ 3. Засоби та заходи захисту інформації від витоку по технічним каналам. (1 бал)	№ 4-5. Порядок створення комплексу технічного захисту інформації на об’єкті інформаційної діяльності. (2 бали)	№ 6. Випробування та атестація КТЗІ. (1 бал)
Практичні, заняття (теми, бали)				№ 1-9 Порядок створення комплексу технічного захисту інформації на об’єкті інформаційної діяльності. (99 балів)	№ 10 Випробування та атестація КТЗІ. (11 балів)
Лабораторні (теми, бали)		№ 1-6 Класифікація технічних каналів витоку інформації. Методи та засоби несанкціонованого отримання інформації по технічним каналам. (66 балів)	№ 7-12 Засоби та заходи захисту інформації від витоку по технічним каналам. (66 балів)		
Самостійна робота	Самостійна робота (5 балів)			Самостійна робота (5 балів)	
Поточний контроль (вид, бали)	Модульна контрольна робота 1 (25 балів)			Модульна контрольна робота 2 (25 балів)	
Підсумковий контроль (вид, бали)	Екзамен (40 балів)				

8. Рекомендовані джерела

Основна (базова):

1. Закон України "Про інформацію".
2. Закон України "Про захист інформації в інформаційно-телекомунікаційних системах".
3. Закон України "Про основи національної безпеки".
4. Закон України «Про основні засади забезпечення кібербезпеки України».
5. УКАЗ ПРЕЗИДЕНТА УКРАЇНИ №447/2021 Про рішення Ради національної безпеки і оборони України від 14 травня 2021 року "Про Стратегію кібербезпеки України"
6. УКАЗ ПРЕЗИДЕНТА УКРАЇНИ №685/2021 Про рішення Ради національної безпеки і оборони України від 15 жовтня 2021 року "Про Стратегію інформаційної безпеки"
7. Постанова Кабінету Міністрів України від 27.11.1998 № 1893 «Про затвердження Інструкції про порядок обліку, зберігання і використання документів, справ, видань та інших матеріальних носіїв інформації, які містять службову інформацію».
8. Порядок захисту державних інформаційних ресурсів в інформаційно-телекомунікаційних системах.
9. ДСТУ 33960-96 Захист інформації. Технічний захист інформації. Основні положення.
10. ДСТУ 33961-96 Захист інформації. Технічний захист інформації. Порядок проведення робіт.
11. ДСТУ 33962-97 Захист інформації. Технічний захист інформації. Терміни та визначення;
12. НД ТЗІ 1.1-005-07 Захист інформації на об’єктах інформаційної діяльності. Створення комплексу технічного захисту інформації. Основні положення.
13. НД ТЗІ 1.4-001-2000. Типове положення про службу захисту інформації в автоматизованій системі.
14. НД ТЗІ 2.5-004-99. Критерії оцінки захищеності інформації в комп'ютерних системах від несанкціонованого доступу.
15. НД ТЗІ 2.5-005-99. Класифікація автоматизованих систем і стандартні функціональні профілі захищеності оброблюваної інформації від несанкціонованого доступу.
16. НД ТЗІ 3.7-003-05. Порядок проведення робіт із створення комплексної системи захисту інформації в інформаційно-телекомунікаційній системі.
17. НД ТЗІ 3.7-001-99. Методичні вказівки щодо розробки технічного завдання на створення комплексної системи захисту інформації в АС.
18. 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.
19. НД ТЗІ 1.6-005-2013 Захист інформації на об’єктах інформаційної діяльності. Положення про категоріювання об’єктів, де циркулює інформація з обмеженим доступом, що не становить державної таємниці.
20. Технічні канали витоку інформації. Порядок створення комплексів технічного захисту інформації: навч. посіб. / С.О. Іванченко, О.В. Гавриленко, О.А. Линський, А.С. Шевцов – К.: ІСЗЗІ НТУУ «КПІ», 2016. – 104 с.

Додаткова:

1. Богуш В.М., Юдін О.К. Інформаційна безпека держави. Навчальний посібник. – К.: "МК-Прес", 2005. – 432 с.
2. Виявлення та блокування негласного отримання інформації на об’єктах інформаційної діяльності: навч. посіб. / О.А. Лаптєв, В.А. Савченко, Г.В. Шуклін – К.: ДУТ, 2020. -126 с.
3. Дослідження комбінаційних характеристик вітчизняних радіо непрозорих тканин М1, М2 та М3 / Ю. Є. Яремчук, В. С. Катаєв, В. В. Сінюгін // Реєстрація, зберігання та обробка даних. – 2015. – Том 17. №3 – С. 56-65.

4. Дослідженняя характеристик вітчизняних радіо непрозорих тканин Н1, Н2 та Н3 при різних комбінаціях їхнього застосування / Ю. Є. Яремчук, В. С. Катаєв, М. Ю. Гижко, П. В. Павловський // Реєстрація, зберігання та обробка даних. – 2016. – Том 18, № 1. – С. 42-51.
5. Технічний захист інформації в інформаційних та телекомунікаційних системах: навч. посіб. / Г.І. Ластівка, П.М. Шпатар – Чернівці: Чернівецький національний університет, 2018. -252 с.
6. Хорошко В.О, Чередниченко В.С., Шелест М.Є. Основи інформаційної безпеки. – К.: ДУІКТ, 2008. – 186 с.

9. Додаткові ресурси

1. Державна служба спеціального зв’язку та захисту інформації [Електронний ресурс]. – Режим доступу: dsszzi.gov.ua