КИЇВСЬКИЙ СТОЛІЧНИЙ УНІВЕРСИТЕТ ІМЕНІ БОРИСА ГРІНЧЕНКА

Факультет інформаційних технологій та математики
Кафедра інформаційної та кібернетичної безпеки
імені професора Володимира Бурячка

«ЗАТВЕРДЖУЮ»
Проректор з наукової роботи
_____ Наталія ВІННІКОВА
«__» січня _____ 2024 р.

РОБОЧА ПРОГРАМА НАВЧАЛЬНОЇ ДИСЦИПЛІНИ

ПРИКЛАДНІ АСПЕКТИ СТВОРЕННЯ ТА ЗАСТОСУВАННЯ СИСТЕМ ТЕХНІЧНОГО ЗАХИСТУ

для аспірантів

спеціальності 125 Кібербезпека та захист інформації
освітнього рівня третього (освітньо-наукового)
освітньо-наукової програми «Інформаційна безпека держави»

Київ – 2024

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 Факультету інформаційних технологій та математики

Протокол від 03.01.2024 № 1

Завідувач кафедри _____ Павло СКЛАДАННИЙ
(підпис)

Робочу програму погоджено з гарантом освітньо-наукової програми «Інформаційна безпека держави»

03.01.2024

Гарант освітньо-наукової програми _____ Наталія КОРШУН
(підпис)

Робочу програму перевірено

11.01.2024

Завідувач аспірантури, докторантури _____ Ілона ТРИГУБ
(підпис)

Пролонговано:

на 20__/20__ н.р. _____ (_____), «____»____ 20___ р., протокол № ___
(підпис) (ПІБ)

на 20__/20__ н.р. _____ (_____), «____»____ 20___ р., протокол № ___
(підпис) (ПІБ)

на 20__/20__ н.р. _____ (_____), «____»____ 20___ р., протокол № ___
(підпис) (ПІБ)

на 20__/20__ н.р. _____ (_____), «____»____ 20___ р., протокол № ___
(підпис) (ПІБ)

1. Опис навчальної дисципліни

Найменування показників	Характеристика дисципліни за формами навчання	
	денна	заочна
Вид дисципліни	обов'язкова	
Мова викладання, навчання та оцінювання	українська	
Загальний обсяг кредитів / годин	3 / 90	
Рік навчання	2	2
Семестр	4	4
Кількість змістових модулів з розподілом:	2	
Обсяг кредитів	3	3
Обсяг годин, в тому числі:	90	90
Аудиторні	24	12
Самостійна робота	60	78
Модульний контроль	6	-
Форма семестрового контролю	залік	залік

2. Мета та завдання дисципліни

Мета: отримання компетентностей зі створення та застосування систем технічного захисту інформації на об'єктах інформаційної діяльності.

Завдання:

− надання аспірантам теоретичних знань про засоби і методи організаційного захисту інформації;

− формування у аспірантів категоріальних понять з принципів побудови систем технічного захисту інформації;

− формування у аспірантів уміння аналізу ефективності систем технічного захисту інформації;

− стимулювання аспірантів до активної аналітико-пошукової роботи, що спрямована на визначення ефективних шляхів застосування систем технічного захисту інформації.

У результаті вивчення навчальної дисципліни відповідно до освітньо-наукової програми спеціальності формуються фахові компетентності:

Програмні компетентості	**Код**	**Значення компетентності**
Спеціальні компетентності	СК 1	Здатність оцінювати фізичні, технологічні, інформаційні, соціологічні, етичні та інші процеси інформаційного і кіберпросторів.
	СК 3	Здатність застосовувати сучасні ІТ технології при створенні систем інформаційної та/або кібербезпеки і захисту інформації, електронні інформаційні ресурси, спеціалізоване програмне забезпечення у науковій та навчальній діяльності; здійснювати проєктну діяльність на засадах лідерства.
	СК 5	Здатність робити оцінки та в умовах припущень і обмежень знаходити відповідні рішення щодо систем інформаційної та/або кібербезпеки і захисту інформації.
	СК 6	Здатність до удосконалення, модернізації та уніфікації систем, засобів і технологій забезпечення безпеки ІТ систем та мереж, обробки та перетворення інформації.
	СК 7	Здатність до планування і реалізації заходів із захисту інформації на об'єктах критичної інфраструктури, проведення моніторингу, аудиту та відновлення процесів штатного функціонування ІТ систем та мереж після збоїв та відмов різних класів і походження.

3. Результати навчання за дисципліною.

У результаті вивчення навчальної дисципліни аспірант повинен:

знати:

– історію та особливості розвитку систем технічного захисту інформації;

– основні процеси що вимагаються при впровадженні систем технічного захисту інформації;

– класифікацію та характеристики апаратних засобів для ефективного впровадження систем технічного захисту інформації;

– основні чинники, що визначають надійність і ефективність систем технічного захисту інформації;

– понятійно-термінологічний апарат в області аналізу та впровадження систем технічного захисту інформації;

вміти:

– визначати тип каналів витоку інформації;

– аналізувати ефективність обраного засобу технічного захисту,

– виявляти особливості систем технічного захисту інформації для різних типів задач;

– обґрунтовувати вибір технічних і організаційних засобів для ефективного впровадження систем технічного захисту інформації;

– визначати ресурси, необхідні для забезпечення надійності функціонування систем технічного захисту інформації з врахуванням факторів помилки у роботі користувачів.

Програмні результати навчання

Код	Значення програмного результату
РН 4	Забезпечувати неперервність бізнес процесів на базі системи управління інформаційною та/або кібербезпекою, згідно вітчизняних та міжнародних вимог і стандартів; здійснювати професійну діяльність на основі знань сучасних інформаційно-комунікаційних технологій, вміти застосовувати їх як в побуті, так і в професійній діяльності; проводити або керувати проведенням наукових і науково-технічних досліджень з питань захисту інформації, організації й забезпечення інформаційної та/або кібербезпеки ОІД; обґрунтовувати раціональні шляхи щодо захисту інформації на ОІД та інформації, що циркулює в ІТ системах та мережах; використовувати сучасні техніки для проведення досліджень за напрямом захисту інформації, організації й забезпечення безпеки мережевої інфраструктури об’єктів інформаційної діяльності, а також наукових досліджень вищих рівнів, зокрема дотичних міждисциплінарних напрямів.
РН 5	Розробляти та аналізувати проєкти ІКС базуючись на стандартизованих технологіях та протоколах передачі даних; аналізувати та визначати можливість застосування технологій, методів та засобів КТЗІ в ІКС; проєктувати та реалізувати комплексні системи КТЗІ в ІКС відповідно до вимог чинних нормативно-правових документів системи захисту інформації; вирішувати задачі впровадження, супроводу та управління комплексними системами захисту інформації в ІКС, проведення їх експертизи та випробувань; забезпечувати процеси захисту інформаційно-комунікаційних систем шляхом встановлення та коректної експлуатації програмних та програмно-апаратних комплексів засобів захисту; використовувати для обґрунтування висновків належні докази, наявні літературні дані.
РН 6	Розробляти та впроваджувати науково-дослідницькі та інноваційні проєкти в сфері захисту інформації, інформаційної та кібербезпеки; розробляти алгоритми, моделі, методи та складні програмні комплекси оцінки характеристик і стану систем інформаційної та кібербезпеки; здійснювати захист ресурсів і процесів в ІКС на основі моделей безпеки та встановлених режимів їх безпечного

	функціонування; забезпечувати процеси захисту інформаційно-комунікаційних систем шляхом встановлення та коректної експлуатації програмних та програмно-апаратних комплексів засобів захисту, виконувати розробку експлуатаційної документації на КЗЗ; забезпечувати функціонування системи управління інформаційною та/або кібербезпекою організації на основі керування інформаційними ризиками з врахуванням можливих конфліктів і катастроф.
РН 7	Вирішувати задачі централізованого і децентралізованого адміністрування доступом до ІР і процесів в ІКС та реалізовувати заходи з протидії отриманню несанкціонованого доступу до них; володіти науково-організаційними основами проведення аудиту безпеки ІКС, а також науковими методами та практичними навичками щодо створення систем моніторингу безпеки в ІТ системах та мережах.

4. Структура навчальної дисципліни

Тематичний план для денної форми навчання

Назва змістових модулів, тем	Усього	Розподіл годин між видами робіт					
		Аудиторні					Самостійна
		Лекції	Семінари	Практичні	Лабораторні	Індивідуальні	
Змістовий модуль 1. Основи створення та застосування систем технічного захисту інформації							
Тема 1. Введення в дисципліну. Основні терміни та визначення. Нормативно-правова база створення систем технічного захисту інформації.	2	2					
Тема 2. Класифікація технічних каналів витоку інформації. Методи та засоби несанкціонованого отримання інформації по технічним каналам.	21	4	2				15
Тема 3. Засоби та заходи захисту інформації від витоку по технічним каналам.	19	2	2				15
Модульний контроль	3						
Разом	45	8	4				30
Змістовий модуль 2. Основні етапи застосування систем технічного захисту інформації на ОІД							
Тема 4. Порядок застосування систем технічного захисту інформації на об’єкті інформаційної діяльності.	23	2		6			15
Тема 5. Випробування та атестація систем технічного захисту інформації.	19	2		2			15
Модульний контроль	3						
Разом	45	4		8			30
Усього	**90**	**12**	**4**	**8**			**60**

Тематичний план для заочної форми навчання

Назва змістових модулів, тем	Усього	Розподіл годин між видами робіт					
		Аудиторна:					Самостійна
		Лекції	Семінари	Практичні	Лабораторні	Індивідуальні	
Змістовий модуль 1. Основи створення та застосування систем технічного захисту інформації							
Тема 1. Введення в дисципліну. Основні терміни та визначення. Нормативно-правова база створення систем технічного захисту інформації.	8						8
Тема 2. Класифікація технічних каналів витоку інформації. Методи та засоби несанкціонованого отримання інформації по технічним каналам.	18	2					16
Тема 3. Засоби та заходи захисту інформації від витоку по технічним каналам.	20	2	2				16
Разом	46	4	2				40
Змістовий модуль 2. Основні етапи застосування систем технічного захисту інформації на ОІД							
Тема 4. Порядок застосування систем технічного захисту інформації на об’єкті інформаційної діяльності.	24	2		2			20
Тема 5. Випробування та атестація систем технічного захисту інформації.	20	2					18
Разом	44	4		2			38
Усього	**90**	**8**	**2**	**2**			**78**

5. Програма навчальної дисципліни

ЗМІСТОВИЙ МОДУЛЬ І. Основи створення та застосування систем технічного захисту інформації.

Тема 1. Введення в дисципліну. Основні терміни та визначення. Нормативно-правова база створення систем технічного захисту інформації.

Введення в дисципліну. Основні терміни та визначення. Термінологія у галузі захисту інформації. Нормативно-правова база створення та застосування систем технічного захисту інформації.

Ключові слова: автоматизована система, нормативний документ системи технічного захисту інформації (НД ТЗІ), комплексна система захисту інформації, правила розмежування доступу.

Література:

1. Про інформацію [Електронний ресурс] : Закон України : чинний від 16.07.2020, підстава 692-IX // База даних «Законодавство України» / ВР України. Режим доступу : https://zakon.rada.gov.ua/laws/show/2657.

2. Про захист інформації в інформаційно-телекомунікаційних системах [Електронний ресурс] : Закон України : чинний від 04.07.2020, підстава 681-IX // База даних «Законодавство України» / ВР України. Режим доступу : https://zakon.rada.gov.ua/laws/show/80.

Тема 2. Класифікація технічних каналів витоку інформації. Методи та засоби несанкціонованого отримання інформації по технічним каналам.

Класифікація та особливості каналів витоку інформації, їх параметри. Перехоплення акустичних сигналів, інформації високочастотного опромінення, побічних електромагнітних випромінювань, зняття інформації за допомогою апаратних закладок, електромагнітні, електричні і індукційні.

Ключові слова: канал витоку інформації, електромагнітне випромінювання, наводка, закладний пристрій, спостереження, розвідка.

Література:

1. Хорошко В.О, Чередниченко В.С., Шелест М.Є. Основи інформаційної безпеки : К.: ДУІКТ, 2008. – 186 с.
2. Богуш В.М., Юдін О.К. Інформаційна безпека держави. Навчальний посібник. –К.: "МК-Прес", 2005. – 432 с.

Тема 3. Засоби та заходи захисту інформації від витоку по технічним каналам.

Організаційні та технічні заходи захисту інформації. Заходи захисту інформації від витоку акустичними, віброакустичними та оптоелектронними каналами, активні та пасивні заходи захисту інформації. Захист інформації від витоку через закладні пристрої.

Ключові слова: співвідношення сигнал/завада, закладні пристрої, звукоізоляція, блокування, маскування, контроль ефективності ТЗІ.

Література:

1. ДСТУ 33960-96 Захист інформації. Технічний захист інформації. Основні положення.
2. НД ТЗІ 2.5-005-99. Класифікація автоматизованих систем і стандартні функціональні профілі захищеності оброблюваної інформації від несанкціонованого доступу.
3. НД ТЗІ 2.5-004-99. Критерії оцінки захищеності інформації в комп'ютерних системах від несанкціонованого доступу.
4. Богуш В.М., Юдін О.К. Інформаційна безпека держави. Навчальний посібник. – К.: "МК-Прес", 2005. – 432 с.

ЗМІСТОВИЙ МОДУЛЬ ІІ. Порядок застосування систем технічного захисту інформації на ОІД.

Тема 4. Порядок застосування систем технічного захисту інформації на об’єкті інформаційної діяльності

Введення СЗІ в дію. Відповідність СЗІ вимогам національних та міжнародних стандартів.

Ключові слова: політика безпеки, політика послуги, автоматизована система, гарантії, диспетчер доступу.

Література:

1. ДСТУ 33961-96 Захист інформації. Технічний захист інформації. Порядок проведення робіт.
2. НД ТЗІ 3.7-003-05. Порядок проведення робіт із створення комплексної системи захисту інформації в інформаційно-телекомунікаційній системі.
3. НД ТЗІ 3.7-001-99. Методичні вказівки щодо розробки технічного завдання на створення комплексної системи захисту інформації в АС.
4. 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.
5. 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.

Тема 5. Випробування та атестація систем технічного захисту інформації

Визначення якості реалізованої системи захисту інформації. Атестація системи захисту інформації. Контроль функціонування і управління системою захисту. Управління системою захисту інформації.

Ключові слова: випробування, атестація, державна експертиза, аудит інформаційної безпеки, експертний висновок, атестат відповідності, технічний паспорт КТЗІ, комплексна перевірка стану ТЗІ.

Література:

1. НД ТЗІ 3.7-001-99. Методичні вказівки щодо розробки технічного завдання на створення комплексної системи захисту інформації в АС.
2. НД ТЗІ 3.7-003-05. Порядок проведення робіт із створення комплексної системи захисту інформації в інформаційно-телекомунікаційній системі.
3. ДСТУ 33961-96 Захист інформації. Технічний захист інформації. Порядок проведення робіт.

6.Контроль навчальних досягнень

6.1. Система оцінювання навчальних досягнень аспірантів (денна форма)

Вид діяльності аспіранта	Максимальна к-сть балів за одиницю	Модуль 1		Модуль 2	
		кількість одиниць	максимальна кількість балів	кількість одиниць	максимальна кількість балів
Відвідування лекцій	1	4	4	2	2
Відвідування практичних занять	1	-	-	4	4
Відвідування семінарських занять	1	2	2	-	-
Робота на практичному занятті	10	-	-	4	40
Робота на семінарському занятті	10	2	20	-	-
Виконання завдань для самостійної роботи	5	3	15	2	10
Виконання модульної роботи	25	1	25	1	25
	Разом	-	66	-	81
Максимальна кількість балів: 147					
Розрахунок коефіцієнта: 100/147=0.68					

Система оцінювання навчальних досягнень аспірантів (заочна форма)

Вид діяльності аспіранта	Максимальна к-сть балів за одиницю	Модуль 1		Модуль 2	
		кількість одиниць	максимальна кількість балів	кількість одиниць	максимальна кількість балів
Відвідування лекцій	1	2	2	2	2
Відвідування практичних занять	1	-	-	1	1
Відвідування семінарських занять	1	1	1	-	-
Робота на практичному занятті	10	-	-	1	10
Робота на семінарському занятті	10	1	10	-	-
Виконання завдань для самостійної роботи	5	3	15	2	10
	Разом	-	28	-	23
Максимальна кількість балів: 51					
Розрахунок коефіцієнта: 100/51=1,96					

6.2. Завдання для самостійної роботи та критерії її оцінювання

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

№ з/п	Назва теми	Кількість годин денна/за очна	Бали
Змістовий модуль 1. Основи створення та застосування систем технічного захисту інформації		30/40	15
1	Нормативно-правова база створення та застосування систем технічного захисту інформації.	-/8	5
2	Класифікація технічних каналів витоку інформації. Методи та засоби несанкціонованого отримання інформації по технічним каналам.	15/16	5
3	Засоби та заходи захисту інформації від витоку по технічним каналам.	15/16	5
Змістовий модуль 2. Основні етапи застосування систем технічного захисту інформації на ОІД		30/38	10
4	Порядок застосування систем технічного захисту інформації на ОІД.	15/20	5
5	Випробування та атестація систем технічного захисту інформації.	15/18	5
	Разом	60/78	25

6.3. Критерії оцінювання самостійної роботи.

№ 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, обґрунтованість власної позиції, пропозиції щодо розв'язання проблеми, визначення перспектив дослідження	2 бали
3	Дотримання вимог щодо технічного оформлення	1 бал
	Разом	5 балів

6.4. Форми проведення модульного контролю та критерії оцінювання

Модульний контроль проводиться у формі контрольної роботи за кожним модулем. Контрольні (модульні) роботи включають тестування, відповіді на теоретичні питання, розв'язання практичних завдань та ситуацій.

Сума балів, накопичених аспірантом за виконання модульних контрольних робіт свідчить про ступінь оволодіння ним програмою навчальної дисципліни на конкретному етапі її вивчення.

Критерії оцінювання модульного контролю з дисципліни наступні:

20-25 балів – у повному обсязі володіє навчальним матеріалом, вільно самостійно та аргументовано його викладає під час відповідей, глибоко та всебічно розкриває зміст теоретичних питань, тестових та практичних завдань.

15-20 балів – достатньо повно володіє навчальним матеріалом, але при викладанні деяких питань не вистачає достатньої глибини та аргументації, допускаються при цьому окремі несуттєві неточності та незначні помилки.

10-15 балів – в цілому володіє навчальним матеріалом та викладає його основний зміст, але без глибокого всебічного аналізу, обґрунтування та аргументації, допускаючи при цьому окремі суттєві неточності та помилки.

1-10 балів – не в повному обсязі володіє навчальним матеріалом, фрагментарно (без аргументації та обґрунтування) його викладає, недостатньо розкриває зміст теоретичних питань та практичних завдань, допускаючи при цьому суттєві неточності.

0 балів – не володіє навчальним матеріалом та не в змозі його викласти, не розуміє змісту теоретичних питань та практичних завдань.

6.5. Форми проведення семестрового контролю.

Семестровий контроль проводиться у вигляді заліку за результатами поточної успішності (проміжного контролю) з усіх змістових модулів дисципліни «Прикладні аспекти створення та застосування систем технічного захисту». Підсумкова семестрова (залікова) рейтингова оцінка аспіранта є сумою підсумкових фактичних оцінок аспіранта за змістовними модулями.

6.6. Оцінювання освітніх досягнень аспірантів за системою ECTS

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

7.Рекомендовані джерела

Основна (базова)

1. Про інформацію [Електронний ресурс] : Закон України : чинний від 16.07.2020, підстава 692-IX // База даних «Законодавство України» / ВР України. Режим доступу : https://zakon.rada.gov.ua/laws/show/2657.
2. Про захист інформації в інформаційно-телекомунікаційних системах [Електронний ресурс] : Закон України : чинний від 04.07.2020, підстава 681-IX // База даних «Законодавство України» / ВР України. Режим доступу : https://zakon.rada.gov.ua/laws/show/80.Закон України "Про основи національної безпеки".
3. Богуш В.М., Юдін О.К. Інформаційна безпека держави. Навчальний посібник. –К.: "МК-Прес", 2005. – 432 с.
4. ДСТУ 33960-96 Захист інформації. Технічний захист інформації. Основні положення.
5. ДСТУ 33961-96 Захист інформації. Технічний захист інформації. Порядок проведення робіт.
6. ДСТУ 33962-97 Захист інформації. Технічний захист інформації. Терміни та визначення.
7. Хорошко В.О, Чередниченко В.С., Шелест М.Є. Основи інформаційної безпеки : К.: ДУІКТ, 2008. – 186 с.

Додаткова

1. НД ТЗІ 1.1-005-07 Захист інформації на об’єктах інформаційної діяльності. Створення комплексу технічного захисту інформації. Основні положення.
2. НД ТЗІ 1.4-001-2000. Типове положення про службу захисту інформації в автоматизованій системі.
3. НД ТЗІ 2.5-004-99. Критерії оцінки захищеності інформації в комп'ютерних системах від несанкціонованого доступу.
4. НД ТЗІ 2.5-005-99. Класифікація автоматизованих систем і стандартні функціональні профілі захищеності оброблюваної інформації від несанкціонованого доступу.
5. НД ТЗІ 3.7-003-05. Порядок проведення робіт із створення комплексної системи захисту інформації в інформаційно-телекомунікаційній системі.
6. НД ТЗІ 3.7-001-99. Методичні вказівки щодо розробки технічного завдання на створення комплексної системи захисту інформації в АС.
7. 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.
8. 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.

Інформаційні джерела:

ДСЗЗІ dsszzi.gov.ua технологій Державна служба спеціального зв’язку та захисту інформації.