Київський університет імені Бориса Грінченка

Факультет інформаційних технологій та управління

Кафедра інформаційної та кібернетичної безпеки

«ЗАТВЕРДЖУЮ»
Проректор з науково-методичної
та навчальної роботи
_____ О.Б. Жильцов
«07» 12 2020 р.

РОБОЧА ПРОГРАМА НАВЧАЛЬНОЇ ДИСЦИПЛІНИ «СИСТЕМИ ТЕХНІЧНОГО ЗАХИСТУ ІНФОРМАЦІЇ»

для студентів

спеціальності	125 Кібербезпека
освітнього рівня	першого (бакалаврського)
освітньої програми	125.00.01 Безпека інформаційних і комунікаційних систем

Київ – 2020

Розробник:

Платоненко Артем Вадимович, старший викладач кафедри інформаційної та кібернетичної безпеки Факультету інформаційних технологій та управління Київського університету імені Бориса Грінченка.

Викладач:

Платоненко Артем Вадимович, старший викладач кафедри інформаційної та кібернетичної безпеки Факультету інформаційних технологій та управління Київського університету імені Бориса Грінченка.

Робочу програму розглянуто і затверджено на засіданні кафедри інформаційної та кібернетичної безпеки

Протокол від 04.09.2019 р. № 8

Завідувач кафедри _____ (підпис) В.Л. Бурячок

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

___.___. 20___ р.

Керівник освітньої програми _____ (підпис) В.В. Семко

Робочу програму перевірено

___.___. 20___ р.

Заступник директора/декана _____ (підпис) І.Ю. Мельник

Пролонговано:

на 2020/2021 н.р. _____ (підпис) (Бурячок В.Л.) (ПІБ), «09» 12 2020 р., протокол № 13

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	4 / 120	
Курс	4	
Семестр	7	
Кількість змістових модулів з розподілом:	2	
Обсяг кредитів	4	
Обсяг годин, в тому числі:	120	
Аудиторні	56	
Модульний контроль	8	
Семестровий контроль	-	
Самостійна робота	56	
Форма семестрового контролю	Залік	

2. Мета та завдання навчальної дисципліни

Робоча навчальна програма з курсу «Системи технічного захисту інформації» є нормативним документом Київського університету імені Бориса Грінченка, який розроблено кафедрою інформаційної та кібернетичної безпеки 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 «Системи технічного захисту інформації» та необхідне методичне забезпечення, складові і технологію оцінювання навчальних досягнень студентів.

Навчальна дисципліна «Системи технічного захисту інформації» складається з двох змістових модулів: Основи технічного захисту інформації, Засоби захисту від витоку технічними каналами. Обсяг дисципліни – 120 год (4 кредити).

Метою викладання навчальної дисципліни «Системи технічного захисту інформації» є отримання компетентностей в області практичного використання технічного забезпечення.

Завдання:

- надання студентам теоретичних знань про системи технічного захисту інформації;
- формування у студентів категоріальних понять з використання СТЗІ;
- формування у студентів уміння аналізу каналів витоку;
- 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:

- ***компетентності у сфері навчання:***
  - здатність до організації самостійної навчальної, практичної та науково-дослідної діяльності;
- ***компетентності у сфері застосування знань в практичних ситуаціях***
  - вміння застосовувати здобуті теоретико-концептуальні професійні знання у процесі практичної роботи;

фахові компетентності:

- ***компетентності у сфері ТЗІ:***
  - глибокі знання та розуміння принципів застосування СТЗІ, необхідного апаратного і організаційного забезпечення для їх використання;
  - уміння аналізувати засоби ТЗІ;
  - здатність до самостійного дослідження на предмет наявності каналів витоку;
- **компетентності у сфері науково-дослідної діяльності:**
  - уміння вивчати і систематизувати знання у галузі ТЗІ;
  - вивчати, узагальнювати й упроваджувати на практиці організаційні засоби ТЗІ.
- **компетентності у сфері вмінь працювати в групі:**
  - здатність використовувати навички взаємодії в роботі, компетентності у сфері навичок міжособистісного спілкування
  - здатність до продуктивного використання комунікації як складової професійної діяльності.

3. Результати навчання за дисципліною

При вивченні курсу «Системи технічного захисту інформації» студенти повинні
знати:

- історію та особливості розвитку СТЗІ;
- основні процеси що вимагаються при використанні засобів ТЗІ;
- класифікацію та характеристики апаратних засобів для ефективного їх впровадження;
- основні чинники, що визначають надійність і ефективність СТЗІ;
- понятійно-термінологічний апарат в області застосування СТЗІ;

уміти:

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

Забезпечує формування наступних компетентностей:
КФ7 – здатність впроваджувати та забезпечувати функціонування комплексних систем захисту інформації;
КФ10 – Здатність застосовувати методи та засоби криптографічного та технічного захисту інформації на ОІД;
Результати навчання:
ПРз 3 - забезпечувати процеси захисту інформаційно-телекомунікаційних (автоматизованих) систем шляхом встановлення та коректної експлуатації програмних та програмно-апаратних комплексів засобів захисту;
ПРз 7 - здійснювати оцінку рівня захищеності інформації що обробляється в ІТС використовувати інструментальні засоби оцінювання наявності потенційних вразливостей.

4. Структура навчальної дисципліни

Тематичний план для денної форми навчання

Назва змістових модулів, тем	Усього	Розподіл годин між видами робіт			
		Аудиторна:			Самостійна
		Лекції	Практичні	Лабораторні	
Змістовий модуль 1. Основи технічного захисту інформації					
Тема 1. Нормативно-правове забезпечення інформаційної безпеки	16	2	2	4	8
Тема 2. Технічні канали витоку інформації	20	4	2	4	10
Тема 3. Організаційно-технічні заходи щодо ТЗІ на об'єкті	20	4	2	4	10
Модульний контроль	4				
Разом	60	10	6	12	28
Змістовий модуль 2. Засоби захисту від витоку технічними каналами					
Тема 4. Методи та засоби блокування технічних каналів витоку інформації	20	4	2	4	10
Тема 5. Методи та засоби для пошуку радіозакладних пристроїв	20	4	2	4	10
Тема 6. Захист електронної інформації	16	2	2	4	8
Модульний контроль	4				
Разом	60	10	6	12	28
Усього	120	20	12	24	56

5. Програма навчальної дисципліни

Змістовий модуль 1. Основи технічного захисту інформації.

Основні питання:

- Поняття технічного захисту інформації, призначення та функції.
- Класифікація технічних каналів витоку інформації.
- Аналіз об'єкту захисту з метою впровадження СТЗІ.

Змістовий модуль 2. Засоби захисту від витоку технічними каналами.

Основні питання:

- Класифікація загальних методів та засобів блокування каналів витоку інформації.
- Основні методи та засоби для практичного пошуку радіозакладних пристроїв.
- Особливості технічного захисту електронної інформації.

6. Контроль навчальних досягнень

Навчальні досягнення студентів з дисципліни оцінюються за модульно-рейтинговою системою, в основу якої покладено принцип поопераційної 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 лабораторних роботах, 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.
- *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.

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	5	5	5	5
Відвідування практичних занять	1	3	3	3	3
Відвідування лабораторних робіт	2	3	6	3	6
Робота на практичному занятті	10	3	30	3	30
Робота на лабораторній роботі	20	3	60	3	60
Виконання завдань для самостійної роботи	5	1	5	1	5
Виконання модульної роботи	25	1	25	1	25
Разом		-	134	-	134
Максимальна кількість балів: 268					
Розрахунок коефіцієнта: 268/100=2,68					

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 технічного захисту інформації		28	5
1	Нормативно-правове забезпечення інформаційної безпеки	8	
2	Технічні канали витоку інформації	10	
3	Організаційно-технічні заходи щодо ТЗІ на об’єкті	10	
Змістовий модуль 2. Засоби захисту від витоку технічними каналами		28	5
4	Методи та засоби блокування технічних каналів витоку інформації	10	
5	Методи та засоби для пошуку радіозакладних пристроїв	10	
6	Захист електронної інформації	8	
	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, обґрунтованість 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 – письмова робота, що складається з 3 запитань (1 та 2 питання – по 5 балів, 3 питання – 15 балів).

Модульна контрольна робота оцінюється у 25 балів.

Критерії оцінювання:

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 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.

Форми проведення семестрового контролю та критерії оцінювання

Семестрове (підсумкове) оцінювання здійснюється у формі заліку, умовою отримання якого є отриманням студентом 60 балів (з врахуванням коефіцієнту) за результатами поточного контролю.

Орієнтовний перелік питань для самоперевірки

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. Надайте визначення ТЗІ.
6. Яке призначення технічного захисту інформації?
7. Надайте визначення поняття технічного каналу витоку інформації.
8. Надайте визначення поняття небезпечного фізичного сигналу.
9. В чому полягає сутність та основні завдання ТЗІ?
10. Що є основними об’єктами захисту інформації?
11. Які технічні засоби і системи звуться додатковими технічними засобами і системами?
12. Яка фізична сутність акустичного сигналу?
13. Яка фізична сутність акустично-електричних перетворень?
14. Які є канали витоку акустичної інформації?
15. Які є види радіозакладних пристроїв?

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 – 20 год., практичні заняття – 12 год., лабораторні – 24 год., модульний контроль – 8 год., самостійна робота – 56 год.

Модулі (назви, бали)	**Змістовий модуль 1. Основи технічного захисту інформації (134 бали)**			**Змістовий модуль 2. Засоби захисту від витоку технічними каналами (134 бали)**		
Лекції (теми, бали)	№ 1 Нормативно-правове забезпечення інформаційної безпеки (1 бал)	№ 2, 3 Технічні канали витоку інформації. (2 бали)	№ 4, 5 Організаційно-технічні заходи щодо ТЗІ на об'єкті (2 бали)	№ 6, 7 Методи та засоби блокування технічних каналів витоку інформації (2 бали)	№ 8, 9 Методи та засоби для пошуку радіозакладних пристроїв. (2 бали)	№ 10 Захист електронної інформації. (1 бал)
Практичні заняття (теми, бали)	№ 1 Нормативна база СТЗІ (11 балів)	№ 2 Аналіз технічних каналів витоку за їх класифікацією (11 балів)	№ 3 Особливості практичного застосування СТЗІ (11 балів)	№ 4 Порівняння технічних засобів блокування каналів витоку (11 балів)	№ 5 Порівняння методів та засобів пошуку радіозакладних пристроїв (11 балів)	№ 6 Аналіз ризиків для електронної інформації (11 балів)
Лабораторні (теми, бали)	№ 1 Основні задачі СТЗІ (22 бали)	№ 2 Основні відмінності технічних каналів витоку (22 бали)	№ 3 Необхідність аналізу технічних каналів витоку на об'єкті (22 бали)	№ 4 Основні пристрої для організації захисту від витоку технічними каналами (22 бали)	№ 5 Застосування технічних засобів для пошуку радіозакладних пристроїв (22 бали)	№ 6 Практичні аспекти ТЗІ (22 бали)
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)		

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. 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».
5. Порядок захисту державних інформаційних ресурсів в інформаційно-телекомунікаційних системах.
6. ДСТУ 33960-96 Захист інформації. Технічний захист інформації. Основні положення.
7. ДСТУ 33961-96 Захист інформації. Технічний захист інформації. Порядок проведення робіт.
8. ДСТУ 33962-97 Захист інформації. Технічний захист інформації. Терміни та визначення;
9. НД ТЗІ 1.1-005-07 Захист інформації на об’єктах інформаційної діяльності. Створення комплексу технічного захисту інформації. Основні положення.
10. НД ТЗІ 1.4-001-2000. Типове положення про службу захисту інформації в автоматизованій системі.
11. НД ТЗІ 2.5-004-99. Критерії оцінки захищеності інформації в комп'ютерних системах від несанкціонованого доступу.
12. НД ТЗІ 2.5-005-99. Класифікація автоматизованих систем і стандартні функціональні профілі захищеності оброблюваної інформації від несанкціонованого доступу.
13. НД ТЗІ 3.7-003-05. Порядок проведення робіт із створення комплексної системи захисту інформації в інформаційно-телекомунікаційній системі.
14. НД ТЗІ 3.7-001-99. Методичні вказівки щодо розробки технічного завдання на створення комплексної системи захисту інформації в АС.
15. 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.
16. 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.

Додаткова:

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.
3. Расторгуев С.П. Основы информационной безопасности. – М.: „Академия”, 2007. – 187 с.
4. Бузов О.О. Защита информации от утечки по техническим каналам. Учебное пособие. М.: Гостехкомисия Росии, 2005. - 435 с.
5. Хорев А.А. Техническая защита информации: учеб. Пособие для студентов вузов. В 3 т. Т.1. Технические каналы утечки информации. – М.: НПЦ "Аналитика", 2008. – 436 с.

9. Додаткові ресурси

1. Державна служба спеціального зв’язку та захисту інформації – Режим доступу: dsszzi.gov.ua
2. Офіційний портал Верховної ради України – Режим доступу: rada.gov.ua
3. Технічний захист інформації – Режим доступу: tzi.ua/ua/tz.html