ХМЕЛЬНИЦЬКИЙ НАЦІОНАЛЬНИЙ УНІВЕРСИТЕТ

Факультет інформаційних технологій

Кафедра Телекомунікацій медійних та інтелектуальних технологій

ЗАТВЕРДЖУЮ
Декан факультету інформаційних технологій
_____ Тетяна ГОВОРУЩЕНКО
05 09 2024 р.

СИЛАБУС

Навчальна дисципліна **Завадостійкість та інформаційна безпека інфокомунікацій**

Освітньо-професійна програма **Електронні інформаційно-комунікаційні системи та мережі**

Рівень вищої освіти **другий (магістерський)**

Загальна інформація

Позиція	Зміст інформації
Викладач(і)	Бойко Юлій Миколайович
Профайл викладача	https://scholar.google.com/citations?user=mQZIGOcAAAAJ&hl=ru 0
E-mail викладача(ів)	boiko_julius@ukr.net
Контактний телефон	0679349960
Сторінка дисципліни в ІСУ	https://msn.khmnu.edu.ua/course/view.php?id=7972
Консультації	**Очні**: вівторок, 6-а пара, 4-236; п'ятниця, 3-а пара, 4-326; **он-лайн:** за необхідністю та попередньою домовленістю

Характеристика дисципліни

Форма навчання	Курс	Семестр	Загальне навантаження		Кількість годин						Курсовий проект	Курсова робота	Форма семестрового контролю	
					Аудиторні заняття				Індивідуальна робота студента	Самостійна робота, в т.ч. ІРС				
			Кредити ЄКТС	Години	Разом	Лекції	Лабораторні роботи	Практичні заняття					Залік	Іспит
ДФН	1	1	5,0	150	51	17	17	17	-	99	-	-	-	+
Разом ДФН			**5,0**	**150**	**51**	**17**	**17**	**17**	**-**	**99**	**-**	**-**	**-**	**1**

Силабус розроблено на основі робочої програми навчальної дисципліни «Програмно-конфігуровані системи передавання, приймання та обробки інформації»

Силабус складено _____ Юлій БОЙКО
Підпис автора — ініціали, прізвище автора

Завідувач кафедри ТМІТ _____ Сергій ПІДЧЕНКО
Підпис — ініціали, прізвище

Хмельницький 2024

Анотація навчальної дисципліни

Інформація, незалежно від того чи становить вона власність держави, суспільства, певних організацій і фірм, а також фізичних осіб, володіє певною цінністю. Звідки можна констатувати, що інформаційні ресурси неодмінно вимагають засобів захисту від різноманітних впливів дія яких може спричинити до руйнування та нівелювання їх цінності. В контексті телекомунікаційних і загалом інформаційно-комунікаційних систем потрібно акцентувати увагу на системах оброки і зберігання даних. Наявність шкідливого і навіть руйнівного програмного забезпечення призводить до ускладнення і унеможливлення усіх базових функцій програмного забезпечення засобів телекомунікацій. Тобто програмні продукти можуть містити приховані функції які можуть бути реалізовані навмисно, які неописані в документації і до яких можна віднести, зокрема, віруси які здатні поширюватись і розмножуватись. Отже, існування сучасних телекомунікаційних і інформаційно-комунікаційних систем в цілому, на сучасному етапі розвитку інформаційних технологій неможливе без застосування спеціальних заходів захисту з метою запобігання пошкодження і руйнування інформації в телекомунікаційних системах.

Дисципліна «Завадостійкість та інформаційна безпека інфокомунікацій» є однією із обов'язкових дисциплін і займає провідне місце у підготовці фахівців освітнього рівня «магістр» за спеціальністю 172 Електронні комунікації та радіотехніка, особливо в контексті підготовки фахівців здатних розуміти і працювати із сучасними телекомунікаційними технологіями. При викладанні дисципліни використовуються активні і творчі форми проведення занять, зокрема оглядові лекції, елементи комп'ютерного моделювання тощо.

Пререквізити: методологія та організація наукових досліджень; програмно-конфігуровані системи передавання, приймання та обробки інформації; ***кореквізити***: апаратно-програмне забезпечення інформаційно-комунікаційних систем та мереж; системний аналіз інформаційно-комунікаційних систем та мереж; моделювання і оптимізація радіотехнічних засобів електронних комунікацій.

Мета і завдання дисципліни

***Мета дисципліни*.** Метою навчальної дисципліни є надання студентам знань, навиків та умінь, щодо методик забезпечення завадостійкості та технологій інформаційного захисту електронних комунікацій, засад інформаційної безпеки, методів технічного захисту інформації в інформаційно-комунікаційних та телекомунікаційних системах, підсистем комплексу засобів захисту, таксономії функцій систем захисту та криптографічних методів захисту інформації.

Завдання дисципліни Формування загальних та спеціальних компетентностей щодо безпекових та інших аспектів функціонування телекомунікаційних та інформаційно-комунікаційних систем; методи підвищення завадостійкості електронних комунікацій; технології інформаційного захисту та програмно-апаратне забезпечення телекомунікаційних систем; методи технічного захисту інформації; принципи криптографічних методів захисту інформації; типові вразливості систем і аналіз причин їх появи; шкідливе програмне забезпечення; нормативні документи з оцінювання захищеності інформації; апаратне забезпечення засобів захисту; передавання інформації через захищені мережі; створення, введення в дію та супроводження захищених систем.

Очікувані результати навчання.

Студент, який успішно завершив вивчення дисципліни, повинен: **розуміти** загальні принципи організації безпекових та інших аспектів функціонування телекомунікаційних та інформаційно-комунікаційних систем, **локалізувати** та оцінювати стан проблемної ситуації на етапах дослідження інформаційної безпеки телекомунікаційних систем, їх проектування, модернізації, впровадження та експлуатації, а також формулювати пропозиції щодо її вирішення з усуненням виявлених недоліків; **забезпечувати** надійність, живучість, завадозахищеність, інформаційну безпеку та пропускну здатність телекомунікаційних та радіотехнічних систем в умовах інформаційних загроз; **розуміти** концептуальні засади та таксономію функцій щодо методів технічного захисту інформації та криптографічних методів захисту інформації; **володіти** навичками застосування нормативних вітчизняних і міжнародних документів (стандартів) з оцінювання захищеності інформації; **опанувати** апаратні та програмні засоби захисту принципи супроводження комплексної системи захисту інформації в телекомунікаційних і інформаційно-комунікаційних системах.

Тематичний план дисципліни і календар його виконання.

Таблиця 3 – ***Тематичний план дисципліни***

№ тижня	**Тема лекції***	**Тема практичного заняття***	**Тема лабораторного заняття***	**Самостійна робота студентів**		
				Зміст	**Год.**	**Література**
1	***2***	***3***	***4***	***5***	***6***	***7***
1	Забезпечення захисту інформації в інформаційно-комунікаційних та телекомунікаційних системах.	Ознайомлення з методами кодування інформації.	Ознайомлення з інструментами по захисту інформації у MS Word	Опрацювання лекційного матеріалу, підготовка до виконання ЛБ 1	14	[**1**] с. 6….21; [**3**] с. 17….31

2	Методика підвищення завадостійкості телекомунікаційних систем. Методи завадостійкого кодування інформації в електронних комунікаціях.	Види шифрів. Ознайомлення з методикою шифрування методом заміни.	Дослідження завадостійкості широкосмугових телекомунікаційних каналів засобами Matlab/Simulink	Опрацювання лекційного матеріалу, підготовка до виконання ПР 1, підготовка до захисту ЛБ 2	14	[**1**] с. 22….50
3	Теоретичні засади захисту інформації. Методи криптографічного захисту інформації в телекомунікаційних і інформаційно-комунікаційних системах.	Вивчення асиметричних криптосистем на основі алгоритму RSA	Визначення пропускної здатності каналів передачі інформації	Опрацювання лекційного матеріалу, підготовка до виконання ПР 2, підготовка до виконанання ЛБ 3	15	[**1**] с. 25….44; [**2**] с. 74….156.
4	Загрози безпеці інформації в програмному забезпеченні телекомунікаційних та інформаційно-комунікаційних системах.	Шифри складної заміни – багатоалфавітні шифри.	Ознайомлення з поняттям захисту інформації та інформаційної безпеки. Визначення критеріїв та аспектів захисту при оцінці інформаційної безпеки	Опрацювання лекційного матеріалу, підготовка до виконання ПР 3, підготовка до виконання ЛБ 4	14	[**1**] с. 62…..72; [2] с. 112….. 148; [**3**] с. 4414…..432
5	Апаратне забезпечення засобів захисту інформації в телекомунікаційних і інформаційно-комунікаційних системах.	Аналіз загроз та методів захисту інформації в інфокомунікаційних системах.	Принципи захисту інформації на основі генератора шуму Базальт - 5 ГЭШ	Опрацювання лекційного матеріалу, підготовка до виконання ПР 4, підготовка до виконання ЛБ 5	14	[**1**] с. 73…..83; [2] с. 399….. 342; [**3**] с. 124…. 148
6	Методи та засоби блокування технічних каналів витоку інформації.	Методики оцінювання захищеності інформації. Стандарти та критерії безпеки інформаційних технологій	Використання радіолокаційної станції ПСНР-1 для захисту інформації та визначення дальності до цілі	Опрацювання лекційного матеріалу, підготовка до виконання ПР 5, підготовка до виконання ЛБ 6	14	[**1**] с. 84-96; [**3**] с. 124-139
7	Методики оцінювання захищеності інформації. Стандарти та критерії безпеки інформаційних технологій.	Заходи щодо інформаційного захисту локальної робочої телекомунікаційної станції.	Ознайомлення з засобами технічного захисту інформації	Опрацювання лекційного матеріалу, підготовка до виконання ПР 6 та 7 підготовка до захисту ЛБ 6 та підготовка до виконання ЛБ 7	14	[**1**] с. 99 ……..103; [**3**] с. 371….. 392

Політика дисципліни.

Організація освітнього процесу в Університеті відповідає вимогам положень про організаційне і навчально-методичне забезпечення освітнього процесу, освітній програмі та навчальному плану. Студент зобов'язаний відвідувати лекції і практичні заняття згідно з розкладом, не запізнюватися на заняття, курсову роботу та інші домашні завдання виконувати відповідно до графіка. Пропущене практичне заняття студент зобов'язаний опрацювати самостійно у повному обсязі і відзвітувати перед викладачем не пізніше, ніж за тиждень до чергової атестації. До практичних занять студент має підготуватися за відповідною темою і проявляти активність.

Критерії оцінювання результатів навчання.

Кожний вид роботи з дисципліни оцінюється за ***чотирибальною*** шкалою. Семестрова підсумкова оцінка визначається як середньозважена з усіх видів навчальної роботи, виконаних і зданих ***позитивно*** з урахуванням коефіцієнта вагомості і встановлюється в автоматизованому режимі після внесення викладачем усіх оцінок до електронного журналу. При оцінюванні знань студентів використовуються різні засоби контролю, зокрема: усне опитування; засвоєння теоретичного матеріалу з тем перевіряється тестовим контролем; якість виконання, набуття теоретичних знань і практичних навичок перевіряється шляхом розв'язання задач та етапів виконання курсового проєкту. Оцінка, яка виставляється за практичне заняття, складається з таких елементів: знання теоретичного матеріалу з теми; вміння студента обґрунтувати прийняті рішення та розв'язувати задачі; своєчасне виконання домашніх завдань з теми.

Структурування дисципліни за видами робіт і оцінювання результатів навчання студентів денної форми навчання у семестрі за ваговими коефіцієнтами

Аудиторна робота		*Самостійна, індивідуальна робота*		*Семестровий контроль*
Захист лабораторної роботи №:		Розв'язок практичних задач:	Контрольна робота	Підсумковий контрольний захід
		ТК1 ТК2	КР	
ВК:	0,20	0,15	0,25	0,4

Оцінювання тестових завдань

Тематичний тест для кожного студента складається з двадцяти п'яти тестових завдань, кожне з яких оцінюється одним балом. Максимальна сума балів, яку може набрати студент, складає 25. Оцінювання здійснюється за чотирибальною шкалою. Відповідність набраних балів за тестове завдання оцінці, що виставляється студенту, представлена у нижченаведеній таблиці.

Сума балів за тестові завдання	1–13	14–16	17–22	23–25
Оцінка за 4-бальною шкалою	2	3	4	5

На тестування відводиться 30 хвилин. Правильні відповіді студент записує у талоні відповідей. Студент може також пройти тестування і в он-лайн режимі у модульному середовищі для навчання MOODLE.

При отриманні негативної оцінки тест слід перездати до терміну наступного контролю.

Співвідношення вітчизняної шкали оцінювання і шкали оцінювання ЄКТС

Оцінка ECTS	**Інституційна шкала балів**	**Інституційна оцінка**		**Критерії оцінювання**
A	4,75-5,00	5	*Зараховано*	**Відмінно** – глибоке і повне опанування навчального матеріалу і виявлення відповідних умінь та навиків.
B	4,25-4,74	4		**Добре** – повне знання навчального матеріалу з кількома незначними помилками.
C	3,75-4,24	4		**Добре** – в загальному правильна відповідь з двома-трьома суттєвими помилками.
D	3,25-3,74	3		**Задовільно** – неповне опанування програмного матеріалу, але достатнє для практичної діяльності за професією.
E	3.00-3,24	3		**Задовільно** – неповне опанування програмного матеріалу, що задовольняє мінімальні критерії оцінювання
FX	2,00-2,99	2	*Незараховано*	**Незадовільно** – безсистемність одержаних знань і неможливість продовжити навчання без додаткових знань з дисципліни
F	0,00-1,99	2		**Незадовільно** – необхідна серйозна подальша робота і повторне вивчення дисципліни.

Орієнтована тематика індивідуального завдання з курсу

1. Телекомунікаційні системи передачі інформації із завадостійким кодуванням
2. Телекомунікаційні системи передачі інформації з криптографічним захистом інформації

3. Захищені системи диспетчеризації та моніторингу рухомих об'єктів на основі використання можливостей GSM та GPS.

4. Захищені системи супутникового доступу до мережі Інтернет

5. Захищені персональної мережі радіодоступу на основі стандартів Bluetooth/ IEEE 802.15.4/ Ad Hoc.

6. Захищені безпроводові локальні мережі на основі стандартів IEEE 802.11 (Wi-Fi)

7. Захищені системи мобільного цифрового потокового IP-телебачення.

8. Захищені міські мережі широкосмугового радіодоступу на основи стандартів (WiMAX, LTE, MIMO)

9. Апаратно-програмні комплекси стиснення відеоінформації на базі алгоритму JPEG та віртуального середовища MATLAB

10. Методи побудови захищених систем електронної комерції та білінгу.

11. Технології захисту інформації у корпоративних мережах великих державних та комерційних організацій з використання програмно-апаратних засобів.

12. Методики побудови захищених мереж на базі технології VIPNet

13. Апаратно-програмні комплекси для вимірювання характеристик мобільних мереж радіодоступу на базі апаратури та програмного забезпечення

14. Закриті та/або скритні системи супутникового зв'язку з використанням розширення спектру методом псевдовипадкової перебудови робочої частоти

15. Захищені цифрові транкінгові системи радіозв'язку на основі стандарту (APCO25, EDACS, Tetrapol, TETRA)

Рекомендований обсяг текстового документа, що готується студентом у процесі виконання індивідуального завдання 20-30 сторінок машинописного тексту формату А4. Для більшої наочності рекомендується широко використовувати таблиці та графічний матеріал – графіки, діаграми з обов’язковими поясненнями до них. Оформлення згідно вимог стандартів Хмельницького національного університету:

- Текстові документи. Загальні вимоги СОУ 207.01:2017/Ю.М. Бойко, Г.В. Красильнікова, Л.І. Першина, Т.Ф. Косянчук. т- Хмельницький : ХНУ, 2017. - 45 с.;

- Бібліографічний запис. Загальні вимоги та правила складання. СОУ 207.02:2017 /Ю.М. Бойко, Л.І. Першина. Хмельницький: ХНУ, 2017. - 37 с.

Контрольні питання з дисципліни.

1. Які з наявних способів реалізації загрози розглядаються в моделі загроз.
2. На порушення яких властивостей інформації та системи спрямована загроза прослуховування трафіку.
3. Наведіть визначення інформаційної безпеки
4. Назвіть об’єкти інформаційної безпеки.
5. Назвіть основні напрями забезпечення безпеки інформації.
6. Які існують базові принципи захисту інформаційних систем.
7. Які рівні захисту інформаційних систем вам відомі.
8. Принципи роботи блокових та потокових шифрів, переваги та недоліки.
9. Призначення, способи генерації та використання ключів.
10. Вимоги до криптосистем та шифрів.
11. Криптографічна стійкість шифрів.
12. Ненадійність ключів та повідомлень.
13. Досконалі шифри.
14. Яка різниця між циклічними кодами і кодами Хемінга.
15. Поясніть реалізацію стохастичних алгоритмів Шеннона-Фано та Хаффмана.
16. Яка особливість декодування при використанні методу LZW.
17. Принципи реалізації алгоритмів з несиметричним ключем.
18. В чому ідея шифрів підстановки.
19. В чому ідея шифрів перестановки.
20. Яка відміна моноалфавітних шифрів від поліалфівітних.
21. На якій ідеї побудований алгоритм RSA.
22. Що таке комп’ютерний вірус. Поняття зараженої програми.
23. Як функціонують антивірусні програми. Класи антивірусних програм.
24. Визначити можливості і недоліки використовуваного брандмауера.
25. Що таке ідентифікація користувачів.
26. Які види ідентифікації вам відомі.
27. Що таке парольна ідентифікація.
28. Що таке аутентифікація користувачів.
29. Чим забезпечується криптостійкість алгоритму
30. Наведіть основні переваги та недоліки асиметричних шифрів.
31. Які засоби контролю використовуються при управлінні безпекою.
32. Які аспекти розглядаються при оцінці ризиків безпеки.
33. Що таке математична модель безпеки.
34. Які моделі безпеки здобули найбільшого поширення.
35. Назвіть основні причини появи вразливостей у сучасних телекомунікаційних і інформаційно-комунікаційних системах.

36. Назвіть типові помилки, що з’являються під час програмної реалізації системи і можуть спричиняти появу вразливостей.

37. Які головні ознаки мережних хробаків, що вирізняють їх з-поміж інших шкідливих програм.

38. Наведіть класифікацію комп’ютерних вірусів.

39. Які програмні засоби дістали назву «троянські коні». Наведіть їх класифікацію.

40. З яких джерел беруть дані для пошуку атак і які можливості мають відповідні сенсори.

41. Методики підвищення завадостійкості телекомунікаційних систем.

42. Методи завадостійкого кодування інформації в електронних комунікаціях.

43. Формування оціночних показників ефективності завадостійкого кодування в електронних комунікаціях.

44. Методика формування та дослідження телекомунікаційного каналу передачі інформації із завадостійким кодуванням.

45 Формування завадостійких сигнально-кодових конструкцій у електронних комунікаціях. Коди з прямим виправленням помилок (FEC). Можливості турбо-кодів, LDPC, полярних кодів у підвищення завадостійкості електронних комунікацій. Канальне кодування.

Рекомендована література

Основна література

1. Бойко Ю.М. Завадостійкість та інформаційна безпека інфокомунікацій : конспект лекцій з дисципліни для здобувачів другого (магістерського) рівня вищої освіти спеціальності 172 «Електронні комунікації та радіотехніка» / Ю. М. Бойко, Л. В. Карпова. Хмельницький : ХНУ, 2024. 111 с.

2. Остапов С. Технології захисту інформації: посібник / С. Остапов, С.П. Євсеєв, О.Г. Король. – Київ : Родовід, 2014. – 428 с.

3. Технології захисту інформації в інформаційно-телекомунікаційних системах [Електронний ресурс] : навчальний посібник / А. В. Жилін, О. М. Шаповал, О. А. Успенський ; КПІ ім. Ігоря Сікорського. – Електронні текстові дані (1 файл: 5,23 Мбайт). – Київ : КПІ ім. Ігоря Сікорського, 2021. – 213 с. – Назва з екрана.

4. Бойко Ю. М. Теоретичні аспекти підвищення завадостійкості й ефективності обробки сигналів в радіотехнічних пристроях та засобах телекомунікаційних систем за наявності завад : монографія / Ю. М. Бойко, В. А. Дружинін, С. В. Толюпа. - Київ : Логос, 2018. - 227 с.

5. Бойко Ю.М. Науково-прикладні питання забезпечення роздільної здатності і ефективності обробки сигналів у радіотехнічних та телекомунікаційних системах за наявності завад : монографія / Ю. М. Бойко, О. М. Шинкарук, Л. В. Карпова, І. І. Чесановський. – Хмельницький : ХНУ, 2019. – 218 с.

6. Хорошко В. О. Проєктування комплексних систем захисту інформації / 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.

7. Buriachok V.L. Methods of information protection in telecommunication systems:[manual]. / V.L.Buriachok, Ie.V.Duravkin, N.V. Lukova-Chuyko, P.M.Skladanniy / – Kiev :KUBG, 2019. – 74 с.

Додаткова література:

1 Богуш В.М. Технічний захист інформації. навч. посіб. / В.М. Богуш, В.Д. Бровко, О.С. Кобус, В.Д. Козюра. - Ліра-К, 2022. – 508 с.

2 Інформаційна безпека : підручник / За ред. Ю. Я. Бобала та І. В. Горбатого. - Видавництво: Львівська політехніка, 2019. – 580 с.

3 Козачок В.А. Політики безпеки. навчальний посібник для студентів вищих навчальних закладів / В.А. Козачок, Г.І. Гайдур, С.О. Гахов, Р.М. Хмелевський, Н.С. Чумак– Київ: ДУТ ННІЗІ, 2020. – 167 с.

4 Бурячок В. Л. Інформаційний та кіберпростори: проблеми безпеки, методи та засоби боротьби. [Посібник]. / В. Л. Бурячок, С.В.Толюпа, В.В.Семко, Л.В.Бурячок, П.М.Складанний Н.В. Лукова-Чуйко/ – Київ : ДУТ - КНУ, 2016. – 178 с.

5 Хорошко В. О. Проєктування комплексних систем захисту інформації / В. О. Хорошко. - Видавництво: Львівська політехніка, 2020. – 320 с.

6 Freeman R. L. Telecommunication System Engineering, 4th Edition / R. L. Freeman. – Wiley, 2015. – 1024 p.

7 Бурячок В.Л. Системний аналіз та прийняття рішень в інформаційній безпеці: підручник. / В.Л. Бурячок, С.В.Толюпа, А.О. Аносов, В.А.Козачок, Н.В. Лукова-Чуйко / – К.:ДУТ, 2015. – 345 с.

8 Вакалюк Т.А. Захист інформації в комп’ютерних системах: навчально-методичний посібник / Т.А. Вакалюк. - Житомир: Вид-во ЖДУ, 2013. – 136 с.

9 Комплексні системи захисту інформації : навчальний посібник / Яремчук Ю. Є., Павловський П. В., Катаєв В. С., Сінюгін В. В. – Вінниця : ВНТУ, 2018. – 118 с.

10 Бойко Ю.М. Інформаційний захист та апаратно-програмне забезпечення телекомунікаційних систем. Завдання та методичні рекомендації до курсового проектування з курсу /Ю.М. Бойко. – Хмельницький: ХНУ, 2022. – 50 с.

Інформаційні ресурси

1. Модульне середовище для навчання (розміщені усі необхідні матеріали з дисципліни, в тому числі тестові завдання для поточного та семестрового контролю знань). http://msn.tup.km.ua/ .

2. Електронна бібліотека університету http://library.tup.km.ua/
3. Репозитарій ХНУ. Доступ до ресурсу: http://elar.khnu.km.ua/jspui/?locale=uk.