Міністерство освіти і науки України

Харківський національний університет імені В.Н. Каразіна

Кафедра безпеки інформаційних систем і технологій

“ЗАТВЕРДЖУЮ”

Проректор

з науково-педагогічної роботи

_____ М.О. Азарєнков

«___» _____ 2020 р.

РОБОЧА ПРОГРАМА НАВЧАЛЬНОЇ ДИСЦИПЛІНИ

Методи синтезу та аналізу захищених телекомунікацій

рівень вищої освіти	третій (освітньо-науковий) рівень
галузь знань	12 Інформаційні технології
спеціальність	125 Кібербезпека
освітня програма	освітньо-наукова програми підготовки докторів філософії
вид дисципліни	вибіркова
факультет	комп’ютерних наук

2020 / 2021 навчальний рік

Програму рекомендовано до затвердження Вченою радою факультету комп'ютерних наук «31» серпня 2020 року, протокол № 12

РОЗРОБНИКИ ПРОГРАМИ:

Завідувач кафедри безпеки інформаційних систем і технологій, доктор технічних наук, доцент **Рассомахін Сергій Геннадійович**

Програму схвалено на засіданні безпеки інформаційних систем і технологій

Протокол від «31» березня 2020 року № 1

Завідувач безпеки інформаційних систем і технологій

_____ Сергій РАССОМАХІН

Програму погоджено з гарантом освітньо-наукової програми 125 «Кібербезпека»

Гарант освітньо-професійної програми «Кібербезпека»

_____ Іван ГОРБЕНКО

Програму погоджено методичною комісією факультету комп'ютерних наук

Протокол від « 31 » серпня 2020 року № 1

Голова методичної комісії факультету комп'ютерних наук

_____ Анатолій БЕРДНІКОВ

ВСТУП

Програма навчальної дисципліни «Методи синтезу та аналізу захищених телекомунікацій» складена відповідно до освітньо-наукової програми підготовки третього (освітньо-наукового) рівня спеціальності 125 Кібербезпека (ВБ 1.1).

1. Опис навчальної дисципліни

1.1. Метою викладання навчальної дисципліни є формування знань, умінь і навичок синтезу структури підсистем інформаційної безпеки та забезпечення цілісності даних, оцінці параметрів захищеності сучасних телекомунікаційних систем та мереж. Вивчення сучасних теоретичних і практичних засад організації і побудови каналів і ліній зв'язку комп'ютерних систем, перетворення форм представлення інформації і даних в каналах багаторівневої цифрової ієрархії, принципів реалізації безпечних мобільних бездротових мереж, систем персонального виклику і транкінгових систем.

1.2. Основними завданнями вивчення дисципліни є формування у студентів певних знань та вмінь з теорії та практики організації захисту інформації від природних та навмисних загроз в мережах інформаційно-комунікаційних систем, навичок аналізу вразливостей і синтезу оптимальних алгоритмів захищених телекомунікацій в багатоканальних системах, а також системах плезіохронної і синхронної ієрархії, мобільних і транкінгових мережах.

1.3 Кількість кредитів - 6

1.4. Загальна кількість годин -180.

1.5. Характеристика навчальної дисципліни	
Нормативна / за вибором	
Денна форма навчання	Заочна (дистанційна) форма навчання
Рік підготовки	
2-й	-й
Семестр	
3-й	-й
Лекції	
16 год.	год.
Практичні, семінарські заняття	
14 год.	год.
Лабораторні заняття	
год.	год.
Самостійна робота	
150 год.	год.
Індивідуальні завдання	
год.	

1.6. Заплановані результати навчання

МАТИ КОМПЕТЕНЦІЇ

Загальні

– **ЗК 5.** Вміння виявляти, ставити та вирішувати проблеми.

Фахові компетентності

– **ФК 1.** Здатність використати сучасні досягнення науки і передових технологій.
– **ФК 5.** Здатність до викладання у вищому навчальному закладі предметів, що відносяться до галузі інформаційно-комунікаційних технологій.
– **ФК 7.** Здатність виконувати роботи з проектування складних комплексів засобів захисту та управління безпекою інформаційних і телекомунікаційних систем відповідно до сфери їх застосування.
– **ФК 8.** Здатність здійснювати та детально обґрунтовувати вибір структури, принципів організації, комплексів засобів і технологій забезпечення безпеки інформаційних і телекомунікаційних систем.

ЗНАТИ:

– основні закономірності та сучасні методи реалізації елементів складних комп'ютерних систем;

– види і характеристики фізичних ліній зв'язку (дротових, оптичних, радіо, радіорелейних, супутникових);

– методи перетворення аналогових форм представлення інформації в цифрові;

– сучасні способи стиснення цифрових потоків;

– принципи організації багатоканального зв'язку і множинного доступу при використанні частотного (FDMA) , часового (TDMA) і кодового (CDMA) розділення абонентів складних комп'ютерних мереж;

– принципи і основні стандарти побудови мереж плезіохронної та синхронної цифрової ієрархії;

– способи і системи реалізації мобільного зв'язку (AMPS, GSM, CDMA, LTE, 5G);

– методи побудови супутникових систем персонального зв'язку (PCSS);

– основні способи реалізації та характеристики транкінгових мереж;

– основні технології і стандарти бездротових мереж, особливості використання мобільних мереж;

– загрози безпеці бездротових мереж, стратегії побудови захищених бездротових мереж.

ВМІТИ:

– проводити інженерну оцінку характеристик ліній зв'язку різної фізичної природи;

– здійснювати розрахунок та моделювання систем перетворення аналогових форм представлення інформації в цифрові;

– практично використовувати методи компактного кодування і стиснення цифрових потоків у складних комп'ютерних мережах;

– розраховувати характеристики і проводити моделювання елементів каналів множинного доступу з частотним і часовим розподілом групового ресурсу;

– проводити аналіз і оптимізацію широкосмугових систем з кодовим розділенням абонентів;

– застосовувати сучасні алгоритми побудови протоколів багаторівневої цифрової ієрархії;

– оцінювати ефективність різних способів організації мобільних мереж;

– виконувати основні операції з проектування та оптимізації характеристик транкінгових систем і систем супутникового зв'язку;

– вміти забезпечувати виконання комплексного захисту інформації від різних видів загроз.

2. Тематичний план навчальної дисципліни

Тема 1. Модель взаємодії відкритих систем.

Склад та функціональне призначення різних рівнів моделі OSI. Класифікація систем електрозв'язку. Класифікація, види і характеристики фізичних ліній зв'язку. Аналогові системи. Цифрові системи передачі даних.

Тема 2. Організація багатоканального зв'язку у комп'ютерних мережах.

Методи багатоканального зв'язку і множинного доступу. Системи з частотним розділенням (FDMA). Системи з часовим розділенням (TDMA). Плезіохронна і синхронна ієрархія. Широкосмугові системи. Системи з кодовим розділенням (CDMA)..

Тема 3. Мобільні мережі, розподілені транкінгові та супутникові системи.

Аналогова телефонія першого покоління NMT-450, AMPS. Мобільні мережі стандарту GSM. Мобільні мережі CDMA (2G LTE, 5G). Системи супутникового зв'язку та персонального виклику. Транкінгові мережі передачі даних. Перспективи розвитку складних комп'ютерних мереж

Тема 4. Принципи побудови бездротових локальних мереж сімейства стандартів IEEE 802.11.

Стек протоколів, архітектура мережі та режими взаємодії її елементів, особливості стандартів. Технології множинного доступу в локальних мережах.

Тема 5. Принципи побудови бездротових мереж широкосмугового доступу сімейства стандартів IEEE 802.16.

Особливості стандартів широкосмугового доступу, архітектура і специфікації мереж, основи управління і організації з'єднань. Технології підвищення якості в мобільних мережах.

3. Структура навчальної дисципліни

Назви розділів і тем	Кількість годин					
	денна форма					
	усього	у тому числі				
		л	п	лаб.	інд.	с. р.
Тема 1. Модель взаємодії відкритих систем.	22	2				20
Тема 2. Організація багатоканального зв'язку у комп'ютерних мережах.	36	4	2			30
Тема 3. Мобільні мережі, розподілені транкінгові та супутникові системи	70	6	4			60
Тема 4. Принципи побудови бездротових локальних мереж сімейства стандартів IEEE 802.11.	26	2	4			20

Тема 5. Принципи побудови бездротових мереж широкосмугового доступу сімейства стандартів IEEE 802.16.	26	2	4			20
Усього годин	**180**	**16**	**14**			**150**

4. Теми практичних занять

№ з/п	Назва теми	Кількість годин
1	Вивчення складу та функціонального призначення протоколів нижчих рівнів моделі Open System Interconnection.	2
2	Математичне моделювання перетворювачів частоти в системах FDMA: простий і балансний модулятори.	2
3	Моделювання генераторів m-послідовностей на основі дзеркальних поліномів.	2
4	Декодування сигналів CDMA на основі квазіортогональних послідовностей Голда.	2
5	Математичне моделювання природних перешкод, що здійснюють загрози цілісності даних в дротових та бездротових мережах.	2
6	Стек протоколів, архітектура мережі та режими взаємодії її елементів, особливості стандартів IEEE 802.11.	2
7	Дослідження особливостей механізмів безпеки та їх ефективності в бездротових персональних мережах стандартів IEEE 802.16.	2
	Разом	**14**

5. Завдання для самостійної роботи

№ з/п	Види, зміст самостійної роботи	Кількість годин
Підготовка до лекцій.		
1	Вивчення елементів формування первинного цифрового потоку (TDMA) в цифрових системах плезіохронної цифрової ієрархії (PDH)	20
2	Вивчення властивостей і імовірнісних характеристик передачі сигналів у стандарті GSM.	20
3	Вивчення характеристик процедури множинного доступу на основі алгоритму ALOHA.	10
4	Методи організації множинного доступу в бездротових мережах.	10
Підготовка до практичних занять		
5	Протоколи, топології мереж, технології доступу в бездротових персональних мережах.	10
6	Особливості стандартів IEEE 802.11, архітектура і специфікації мереж, основи управління і організації з’єднань.	20
7	Основні заходи безпеки в супутникових та цифрових транкінгових мережах.	20
8	Вразливість технологій автентифікації та WEP-шифрування в мережах 802.11, підвищення рівня безпеки за рахунок використання різних алгоритмів шифрування.	20
Читання додаткової літератури		20
	Разом	**150**

6. Індивідуальні завдання

/Не передбачено/

7. Методи контролю

Поточний контроль здійснюється протягом семестру. Здобувачі отримують оцінки за кожне з практичних завдань за чотири рівневою шкалою, контрольна робота. Сумарна оцінка поточного семестрового контролю нормується на 60 балів

Максимальна кількість балів за результатами контролю поточної успішності складає 100 балів.

Таблиця 7.1 – Розподіл балів, які отримують аспіранти за результатами контролю поточної успішності

Вид заняття / контрольний захід	**Оцінка** N_{max}
Практичні заняття	
ПЗ 1	10
ПЗ 2	10
ПЗ 3	10
ПЗ 4	20
ПЗ 5	20
ПЗ 6	20
ПЗ 7	10
Всього за семестр	100

Згідно рішення кафедри безпеки інформаційних систем і технологій до заліку не допускаються аспіранти, що не захистили звіті з практичних занять.

Підсумковий контроль здійснюється за результатами поточного контролю шляхом підсумовування оцінок, отриманих за практичні заняття.

8. Схема нарахування балів

Підсумковий семестровий контроль в формі заліку без виконання залікової роботи

Поточний контроль, самостійна робота, індивідуальні завдання					Сума
Розділ 1					
Т1	Т2	Т3	Т4	Т5	100
20	20	20	20	20	

Шкала оцінювання

Сума балів за всі види навчальної діяльності протягом семестру	Оцінка для дворівневої шкали оцінювання
90 – 100	Зараховано
70-89	
50-69	
1-49	Незараховано

Критерії оцінювання

Критерії оцінювання знань студентів за виконання практичних занять

Визначення	Кількість балів*
Завдання з практичного заняття виконане самостійно в повному обсязі. Звіт оформлений	N_{max}

акуратно відповідно до вимог методичних вказівок. При захисті звіту показано розуміння суті і змісту проведених досліджень	
Завдання з практичного заняття виконане самостійно в повному обсязі. Звіт оформлений достатньо акуратно відповідно до вимог методичних вказівок. При захисті звіту були виявлені незначні помилки у знанні теоретичного матеріалу.	$[N_{max} - \left\lfloor \frac{N_{max}}{4} \right\rfloor, N_{max} - 1]$
Завдання з практичного заняття виконане в повному обсязі. Звіт оформлений достатньо акуратно, в оформленні звіту є незначні недоліки. При захисті звіту були виявлені незначні помилки у знанні теоретичного матеріалу.	$[N_{max} - 2 \times \left\lfloor \frac{N_{max}}{4} \right\rfloor, N_{max} - \left\lfloor \frac{N_{max}}{4} \right\rfloor - 1]$
Завдання з практичного заняття виконане. Звіт оформлений з помилками і недоліками. При захисті звіту були виявлені суттєві помилки у знанні теоретичного матеріалу.	$[N_{max} - 3 \times \left\lfloor \frac{N_{max}}{4} \right\rfloor, N_{max} - 2 \times \left\lfloor \frac{N_{max}}{4} \right\rfloor - 1]$
Показано недосконале знання навчального матеріалу, допущені суттєві помилки, які носять принциповий характер. Звіт оформлений з помилками і суттєвими недоліками.	$[1, N_{max} - 3 \times \left\lfloor \frac{N_{max}}{4} \right\rfloor - 1]$

* N_{max} – максимальна кількість балів для відповідного заняття відповідно до таблиці 7.1.

9. Рекомендована література

9.1 Основна література

1. Rassomakhin, S.G. Mathematical and physical nature of the channel capacity. Telecommunications and Radio Engineering, 2017, 76(16), p. 1423-1451.

2. Томаси У. Электронные системы связи. М.: Техносфера, 2007.–1360 с.

3. Скляр Б. Цифровая связь. Теоретические основы и практическое применение. Изд-е 2-е, испр.: Пер с англ.–М.: "Вильямс", 2003.–1104 с.

4. Гаранин М.В., Журавлев В.И., Кунегин С.В. Системы и сети передачи информации.–М.: Радио и связь,2001.–336 с.

5. Столлингс В. Беспроводные линии связи и сети. - М. : Издательский дом «Вильямс», 2003. - 638 с.

6. Педжман Рошан, Джонатан Лиэри Основы построения беспроводных локальных сетей стандарта 802.11 : Пер. с англ. - М.: Издательский дом «Вильямс», 2004. - 304 с.

7. Мерритт Максим, Дэвид Поллино Безопасность беспроводных сетей. - М.: ДМК пресс, Компания АйТи, 2004.-244 с.

8. Shannon C. E. A Mathematical Theory of Communication / Shannon C. E. // Bell Syst. Tech., July-October, 1948. – Vol. 27. – P. 379-423, 623-656.

9. Verdu S. Fifty Years of Shannon Theory / IEEE Transactions on Information Theory, Vol. 44, № 6, October 1998. – pp. 2057 – 2078.

10. И.В. Шахнович Современные технологии беспроводной связи. Издание второе, исправленное и дополненное. - М.: Техносфера, 2006. – 288с.

9.2 Допоміжна література:

1. Вишневский В.М., Ляхов А.И., Портной С.Л., Шахнович И.В. Широкополосные беспроводные сети передачи информации. – М.: Техносфера, 2005. –592 с.
2. Шахнович И.В. Современные технологии беспроводной связи. –М.: Техносфера, 2006.– 288 с.
3. Величко В.В. Передача данных в сетях мобильной связи третьего поколения. – М.: Радио и связь, 2005.– 332 сс.
4. Гепко И.А., Олейник В.Ф., Чайка Ю.Д., Бондаренко А.В. Современные беспроводные сети: состояние и перспективы развития. – К.: «ЭКМО», 2009. - 672 с.
5. James Kempf Wireless Internet Security Architecture and Protocols. – New York: Cambridge University Press, 2008. – 212 p.
6. William Stallings CRYPTOGRAPHY AND NETWORK SECURITY. PRINCIPLES AND PRACTICE.FIFTH EDITION. - Pearson Education, Inc., publishing as Prentice Hall, 2011. – 721 p.

10. Посилання на інформаційні ресурси в Інтернеті, відео-лекції, інше методичне забезпечення

1. Технологія PDH (Плезіохронна цифрова ієрархія). https://skomplekt.com/technology/pdh.htm/

2. Синхронна цифрова ієрархія (SDH). http://its.kpi.ua/ts/SiteAssets/SitePages/files_noskov/%D0%9C%D0%BE%D0%B4%D1%83%D0%BB%D1%8C%204.%20%D0%A1%D0%B8%D0%BD%D1%85%D1%80%D0%BE%D0%BD%D0%BD%D0%B0%D1%8F%20%D1%86%D0%B8%D1%84%D1%80%D0%BE%D0%B2%D0%B0%D1%8F%20%D0%B8%D0%B5%D1%80%D0%B0%D1%80%D1%85%D0%B8%D1%8F%20(SDH).pdf

3. Sergey G. Rassomakhin (April 30th 2019). Digital Algebraic Method for Processing Complex Signals for Radio Monitoring Systems [Online First], IntechOpen, DOI: 10.5772/intechopen.85590. Available from: https://www.intechopen.com/online-first/digital-algebraic-method-for-processing-complex-signals-for-radio-monitoring-systems

4. Протоколы безопасности телекоммуникационных сетей http://www.hups.mil.gov.ua/periodic-app/article/9929/soi_2012_6_27.pdf

3. Телекоммуникационные и информационные сети http://www.dut.edu.ua/ru/lib/1/category/889