Харківський національний університет імені В.Н. Каразіна
Факультет комп'ютерних наук
Кафедра безпеки інформаційних систем і технологій

Ухвалено
Вченою радою
факультету комп'ютерних наук
Протокол № 12 від 31.08.2020
Голова Вченої ради

Назва курсу	Методи синтезу та аналізу захищених телекомунікацій
Викладач (-і)	Завідувач кафедри БІСТ Рассомахін С.Г.
Профайл викладача (-ів)	http://www-csd.univer.kharkov.ua/about-us/sub-faculty/kafedra-bezpeki-informatsijnih-sistem-i/personalnij-sklad/
Контактний тел.	Кафедра: (057) 705-10-83
E-mail:	rassomakhin@karazin.ua
Сторінка курсу в системі дистанційного навчання	Email: rassomakhin@karazin.ua Skype: live: sgrass57_1
Консультації	*Очні консультації*: розклад в університеті (на кафедрі). *Он лайн консультації*: через e-mail та Skype.

1. Коротка анотація до курсу

Курс спрямований на ознайомлення аспірантів з основними методами синтезу та аналізу процесів і протоколів при обміні інформацією в умовах дії природних та навмисних загроз цілісності, конфіденційності та доступності даних. Основна увага при навчанні приділяється вивченню шляхів реалізації сучасних систем плезіохронної та синхронної ієрархії та систем розподілення фізичних ресурсів багатоканальних систем передачі інформації.

2. Мета та цілі курсу

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.

Основні цілі курсу – формування у аспірантів певних знань та вмінь з:

- практики організації захисту інформації від природних та навмисних загроз в мережах ІКС;
- аналізу вразливостей і синтезу оптимальних алгоритмів захищених телекомунікацій;
- принципів побудови і оптимізації багатоканальних систем;
- загальних та спеціальних засад плезіохронної та синхронної ієрархії в глобальних системах обміну даними;
- аналізу і синтезу структури транкінгових систем;
- синтезу та оцінці захищеності систем сповіщення та персонального виклику;
- математичного моделювання елементів багатоканальних систем;

- аналізу загроз інформаційної безпеки у складних розподілених системах;
- формулювання наукових висновків з аналізу сучасних досягнень у галузі захищених комунікацій.

3. Формат курсу – очний.

4. Результати навчання

За результатами вивчення дисципліни аспіранти повинні ЗНАТИ:

- основні закономірності та сучасні методи реалізації елементів складних ІКС;
- 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.

5. Обсяг курсу

Вид заняття	Загальна кількість годин
Лекції	16
Семінарські заняття / практичні / лабораторні	14
Самостійна робота	150
Разом:	180

6. Ознаки курсу:

Рік викладання	Семестр	Спеціальність	Курс (рік навчання)	Нормативний / вибірковий
2020	3	125 Кібербезпека	2	Вибірковий

7. Пререквізити

Попередньо прослухані курси: Теорія інформації, Основи теорії передачі інформації, Компоненти складних комп'ютерних мереж (підготовка бакалаврів за спеціальністю 125 або іншою з галузі знань 12 – інформаційні технології), Математичні основи проектування і оптимізації інформаційно-комунікаційних систем (підготовка магістрів за спеціальністю 125 або іншою з галузі знань 12 – інформаційні технології), Підготовка наукових публікацій та презентація результатів досліджень, Математичні методи в кібербезпеці (підготовка докторів філософії за спеціальністю 125).

8. Технічне та програмне забезпечення /обладнання

Для виконання практичних робіт студентам знадобляться персональні комп'ютери.

9. Політики курсу

Політика доброчесного навчання та стимулювання: передбачає бонуси (додаткові бали за творчо інноваційно виконані завдання) та штрафи (позбавлення відповідних балів за невиконані завдання та пропуск занять без поважних причин).

Політика академічної доброчесності: виконання завдань за персональними варіантами та вхідними даними, що виключає можливість використання чужих результатів.

10. Схема курсу

Тиж. / акад. год.	**Тема, план, короткі тези**	**Форма діяльності (заняття)* / Формат****	**Матеріали**	**Завдання, год**
Тиж. 1 / 2 год.	Тема 1. Л.1. Вступ. Модель взаємодії відкритих систем. Вимоги до рівнів та їх функціональне призначення.	Лекція / (*аудиторна*)	Презентація лекції.	Переглянути презентацію, 2 год. Самостійно: Ознайомитись з моделлю OSI, додатковою літературою, 20 годин.
Тиж. 2 / 2 год	Тема 2. Л.2. Організація багатоканального зв'язку у комп'ютерних мережах.	Лекція / *аудиторна*	Презентація лекції.	Ознайомитись з літературою, переглянути презентацію, 2 год. Самостійно: вивчити історію багатоканального зв'язку, 10 год.
Тиж.3 / 2 год	Тема 2. Л.3. Принципи частотного, часового та кодового розподілу ресурсів.	Лекція / *аудиторна*	Презентація лекції.	Ознайомитись з літературою, переглянути презентацію, 2 год. Самостійно: вивчити методи перетворювання частоти, та розподілу часу у групових трактах, 10 год.

Тиж.4 / 2 год	Тема 2. ПЗ.1. Вивчення складу та функціонального призначення протоколів нижчих рівнів моделі Open System Interconnection..	Практичне заняття / аудиторне	Методичні рекомендації.	Виконати завдання до ПЗ, 2 год. Самостійно: функції протоколів фізичного та канального рівнів OSI, 10 год.
Тиж. 5 / 2 год	Тема 3. Л.4. Мобільні мережі. Системи AMPS, GSM/	Лекція / *аудиторна*	Презентація лекції.	Ознайомитись з літературою, переглянути презентацію, 2 год. Самостійно: мережі першого та другого поколінь, 10 год.
Тиж. 6 / 2 год	Тема 3. Л.5. Мобільні мережі. Системи 4G, LTE, 5G.	Лекція / *аудиторна*	Презентація лекції.	Ознайомитись з літературою, переглянути презентацію, 2 год. Самостійно: розподіл ресурсу при множинному доступі у стандартах 4G і 5G, 10 год.
Тиж. 7 / 2 год	Тема 3. Л6. Мобільні мережі. Розподілені транкінгові та супутникові системи	Лекція / *аудиторна*	Презентація лекції.	Ознайомитись з літературою, переглянути презентацію, 2 год. Самостійно: структура та протоколи TETRA, 10 год.
Тиж. 8 / 2 год	Тема 3. ПЗ 2. Математичне моделювання перетворювачів частоти в системах FDMA: простий і балансний модулятори.	Практичне заняття / аудиторне	Методичні рекомендації.	Виконати завдання до ПЗ, 2 год. Самостійно: вивчити методи моделювання перетворювачів частоти модуляцією, 16 год.
Тиж. 9 / 2 год	Тема 3. ПЗ 3. Моделювання генераторів m-послідовностей на основі дзеркальних поліномів.	Практичне заняття / аудиторне	Методичні рекомендації.	Виконати завдання до ПЗ, 2 год. Самостійно: вивчити математичні основи генераторів на основі LFSR, 14 год.
Тиж. 10 / 2 год	Тема 4. Л.7. Принципи побудови бездротових локальних мереж сімейства стандартів IEEE 802.11..	Лекція / *аудиторна*	Презентація лекції.	Ознайомитись з літературою, переглянути презентацію, 2 год. Самостійно: Вивчити номенклатуру стандартів IEEE 802.11, 4 год.
Тиж. 11 / 2 год	Тема 4. ПЗ.4. Декодування сигналів CDMA на основі квазіортогональних послідовностей Голда.	Практичне заняття / аудиторне	Методичні рекомендації.	Виконати завдання до ПЗ, 2 год. Самостійно: вивчити принципи квазіортогонального кодування, 8 год.
Тиж. 12 / 2 год	Тема 4. ПЗ 5. Математичне моделювання природних перешкод, що здійснюють загрози цілісності даних в дротових та бездротових мережах.	Практичне заняття / *аудиторне*	Методичні рекомендації.	Виконати завдання до ПЗ, 2 год, Самостійно: моделі шумів Котельникова і Шеннона, 8 год.

Тиж. 13 / 2 год	Тема 5. Л.8. Принципи побудови бездротових мереж широкосмугового доступу сімейства стандартів IEEE 802.16.	Лекція / аудиторна	Презентація лекції.	Ознайомитись з літературою, переглянути презентацію, 2 год. Самостійно Вивчити номенклатуру стандартів IEEE 802.16, 4 год.
Тиж. 14 / 2 год	Тема 5. ПЗ. 6. Стек протоколів, архітектура мережі та режими взаємодії її елементів, особливості стандартів IEEE 802.11..	Практичне заняття / *аудиторне*	Методичні рекомендації.	Виконати завдання до ПЗ, 2 год. Самостійно: типи сигналів та розподілу ресурсу 802.11, 8 год.
Тиж. 15 / 2 год	Тема 5. ПЗ. 7. Дослідження особливостей механізмів безпеки та їх ефективності в бездротових персональних мережах стандартів IEEE 802.16.	Практичне заняття / *аудиторне*	Методичні рекомендації.	Виконати завдання до ПЗ, 2 год. Самостійно: захист від атак на протоколи бездротового доступу, 8 год.

11. Система оцінювання та вимоги

Загальна система оцінювання курсу	участь в роботі впродовж семестру – 100 балів. Розподіл балів, що присвоюються аспірантам з навчальної дисципліни «Методи синтезу та аналізу захищених телекомунікацій», є сумою балів за виконання всіх практичних завдань.
Практичні заняття	Аспірант отримує максимальну кількість балів за практичне завдання, якщо: завдання виконане повністю та без допомоги викладача; аспірант самостійно може узагальнити, систематизувати матеріал та вільно застосовує його у стандартних ситуаціях та у ситуаціях невизначеності.
Умови допуску до підсумкового контролю	Виконання та захист всіх практичних завдань.

Розподіл балів, які отримують аспіранти за результатами контролю поточної успішності

Вид заняття / контрольний захід	Кількість балів (*Nmax*)
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

Схема нарахування балів

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

Критерії оцінювання

Критерії оцінювання знань студентів за виконання практичних занять

Визначення	Кількість балів*
Завдання з практичного заняття виконане самостійно в повному обсязі. Звіт оформлений акуратно відповідно до вимог методичних вказівок. При захисті звіту показано розуміння суті і змісту проведених досліджень.	20(10)
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.	15-19(8-9)
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.	10-14(5-7)
Завдання з практичного заняття виконане. Звіт оформлений з помилками і недоліками. При захисті звіту були виявлені суттєві помилки у знанні теоретичного матеріалу.	6-9(3-4)
Показано недосконале знання навчального матеріалу, допущені суттєві помилки, які носять принциповий характер. Звіт оформлений з помилками і суттєвими недоліками.	1-5(1-2)

Шкала оцінювання

Сума балів за всі види навчальної діяльності протягом семестру	Оцінка
	для дворівневої шкали оцінювання
50 – 100	зараховано
1-49	не зараховано

12. Рекомендована література 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. Bernard Sklar Digital communications. Fundamentals and Applications. Second Edition. Prentice Hall, Inc., 2001.
3. Gerry Howser Computer Networks and the Internet. Springer Nature Switzerland AG, 2020.
4. Matt Bishop Computer Security Art and Science.Second Edition. - Pearson Education, Inc., 2019.
5. Emerging security algorithms and techniques / editors, Khaleel Ahmad and oth. - Taylor & Francis, 2019.

6. Shannon C. E. A Mathematical Theory of Communication / Shannon C. E. // Bell Syst. Tech., JulyOctober, 1948. – Vol. 27. – P. 379-423, 623-656.
7. Verdu S. Fifty Years of Shannon Theory / IEEE Transactions on Information Theory, Vol. 44, № 6, October 1998. – pp. 2057 – 2078.
8. Design and Analysis of Security Protocol for Communication. Edited by Dinesh Goyal and oth. - Scrivener Publishing LLC, 2020.

Допоміжна література

1. James Kempf Wireless Internet Security Architecture and Protocols. – New York: Cambridge University Press, 2008. – 212 p.
2. William Stallings Cryptography and network security. Principles and practice.fifth edition. - Pearson Education, Inc., publishing as Prentice Hall, 2011. – 721 p.

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/digitalalgebraic-method-for-processing-complex-signals-for-radio-monitoring-systems
4. CERT-UA - Урядова команда реагування на комп'ютерні надзвичайні події України: https://cert.gov.ua/
5. Computer Security Resource Center : https://csrc.nist.gov/