

Силабус навчальної дисципліни
Безпека інфокомунікаційних мереж

В.А. Золотарьов,
 доцент. каф. ІМІ, к.т.н., доцент
 E-mail: vadym.zolotarov@nure.ua

Назва поля	Детальний контент, коментарі
Назва факультету	Факультет інфокомунікацій
Рівень вищої освіти	Перший (бакалаврський)
Код і назва спеціальності	172 Телекомунікації та радіотехніка
Тип і назва освітньої програми	ОПП «Інформаційно-мережна інженерія»»
Назва дисципліни	Безпека інфокомунікаційних мереж
Кількість ЄКТС кредитів	5
Структура дисципліни (розподіл за видами та годинами навчання)	28 год – 14 лекцій, 8 год – 5 практичних заняття, 20 год – 5 лабораторних заняття, 8 год – 4 консультацій, 71 год – самостійна робота, вид контролю: залік
Графік (терміни) вивчення дисципліни	4-й рік, VII семестр
Передумови для навчання за дисципліною	Раніше мають бути вивчені дисципліни «Основи інформаційно-комунікаційних технологій»; «Основи схемотехніки;» Вища математика (спецрозділи); «Напрямні системи електричного та оптичного зв'язку»; «Технології обробки даних в ІК»; «Локальні мережі зв'язку»; «Системи мобільного зв'язку»
Компетентності, знання, вміння, розуміння, якими оволодіє здобувач вищої освіти в процесі навчання	вміти забезпечувати конфіденційність особистої та службової інформації за допомогою отримання теоретичних знань та практичних навиків; користуватися нормативно-правовою базою у галузі інформаційної безпеки; визначати інформацію, що підлягає захисту; впроваджувати і використовувати обрані заходи забезпечення інформаційної безпеки; використовувати свої теоретичні знання та практичні навички для виявляти загрози інформації; аналізувати інформаційні ризики; здійснювати вибір засобів захисту. Володіти в процесі практичної діяльності в галузі інфокомунікацій навичками по забезпечуванню інформаційної безпеки мережі; вибору апаратно-технічного, криптографічного та програмного забезпечення для конкретної мережі; вміти виявляти та перекривати технічні канали витоку інформації.
Якість освітнього процесу	Навчально-методичне та матеріально-технічне ресурсне забезпечення освітньої програми, в рамках якої проводиться вивчення дисципліни, відповідає ліцензійним вимогам та акредитаційним умовам провадження освітньої діяльності університету. Здійснюється щорічний моніторинг та перегляд навчальної програми дисципліни у відповідності до вимог та

	<p>рекомендацій МОН, державної атестації щодо набутих компетентностей випускників, стандартів співпраці з роботодавцями щодо забезпечення конкурентоспроможного рівня підготовки фахівців. Дотримання принципів академічної доброчесності (https://lib.nure.ua/plagiat). Містить публічну інформацію щодо вимог, компетенцій, рівня освіти в рамках дійсної освітньої програми.</p>
--	---

Опис та зміст дисципліни

Мета вивчення дисципліни - здобування знань, навичок і прийомів роботи з програмними та апаратними засобами захисту інформації, такими як криптографічні пакети, програмно-апаратні комплекси мережного захисту, антивірусне програмне забезпечення та інше; здобування спеціальних знань та практичних навичок у використанні сучасних інформаційних технологій у професійній діяльності.

Зміст

Змістовний модуль 1. Теоретичні основи інформаційної безпеки телекомунікаційних систем

Тема 1. Інформаційна безпека телекомунікаційних систем: сутність, чинники, критерії

Тема 2. Методи захисту інформації в телекомунікаційних системах

Тема 3. Нормативно-правова база захисту інформації в телекомунікаційних системах.

Змістовний модуль 2. Криптографічний захист інформації

Тема 1. Криптографія: основні поняття та визначення

Тема 2. Класична криптографія: шифри підстановки, шифри простої та складної заміни

Тема 3. Блокові симетричні методи шифрування

Тема 4. Асиметричні методи шифрування

Тема 5. Методи автентифікації інформації в телекомунікаційних системах

Тема 6. Електронний цифровий підпис

Змістовний модуль 3. Системи захисту інформації в телекомунікаційних системах

Тема 1. Захист інформації від витоку технічними каналами в телекомунікаційних системах

Тема 2. Захист інформації в стаціонарних телефонних лініях

Тема 3. Методи та засоби захисту інформації в системах рухомого зв'язку

Тема 4. Апаратно-технічні засоби захисту телекомунікаційних систем

Тема 5. Програмні методи захисту інформації в телекомунікаційних системах

Тема 6. Стеганографія

Результати навчання здобувача вищої освіти

За результатом вивчення дисципліни студенти повинні:

Знати: основні тенденції розвитку інформаційно –телекомунікаційних, загрози інформації; можливості витоку інформації у каналах зв'язку; застосування технологій по захисту інформації в телекомунікаціях; нормативно-правову базу використання технічних та програмних засобів захисту інформації в телекомунікаціях, стаціонарному та рухомому зв'язку; види захисного програмного забезпечення та їх призначення; криптографічні засоби захисту інформації; можливості використання програмних засобів для обмеження доступу до електронних документів як на локальному ПК так і через інформаційно-комунікаційну мережу, за допомогою стандартних засобів шифрування інформації;

Вміти: забезпечувати конфіденційність особистої та службової інформації за допомогою отримання теоретичних знань та практичних навиків; користуватися нормативно-правовою базою у галузі інформаційної безпеки; визначати інформацію, що підлягає захисту; впроваджувати і використовувати обрані заходи забезпечення інформаційної безпеки; використовувати свої теоретичні знання та практичні навички для виявляти загроз інформації; аналізувати інформаційні ризики; здійснювати вибір засобів захисту.

Володіти в процесі практичної діяльності в галузі інфокомунікацій навичками по забезпечуванню інформаційної безпеки мережі; вибору апаратно-технічного, криптографічного та програмного забезпечення для конкретної мережі; вміти виявляти та перекривати технічні канали витоку інформації.

Система оцінювання відповідно до кожного завдання для складання заліку/екзамену

Для оцінювання роботи студента протягом семестру підсумкова рейтингова оцінка $O_{сем}$ розраховується як сума оцінок за різні види занять та контрольні заходи

Види занять / контрольний захід	Оцінка
Лабораторні роботи № 1, 2	$(6...10) \times 2 = 12...20$
Практичні роботи № 1, 2,3	$(3...5) \times 3 = 9...15$
Контрольна робота №1	$(3...5) = 3...5$
Контрольна точка № 1	24...40
Лабораторні роботи № 3, 4, 5	$(6...10) \times 3 = 18...30$

Практичні роботи № 1, 2,3	$(3...5) \times 2 = 6...10$
Контрольна робота №1	$(3...5) = 3...5$
Практичне контрольне завдання № 1, 2, 3	$(3...5) \times 3 = 9...15$
Контрольна точка № 2	36...60
Разом	60...100

Як форма підсумкового контролю для дисципліни ЗІТКС використовується письмовий (комбінований) іспит. При цьому виді контролю підсумкова оцінка P_n обчислюється за формулою:

$$P_n = 0,6 Q_{сем} + 0,4 Q_{ісп},$$

де $Q_{сем}$ – оцінка за семестр у 100-бальній системі,
 $Q_{ісп}$ - оцінка за іспит у 100-бальній системі.

Білет для іспиту складається з 2-х теоретичних питань та однієї задачі. Теоретичне запитання оцінюється в 30 балів, а задача – у 30 балів (в сумі – 100 балів).

Якісні критерії оцінювання в національній шкалі та ECTS

Критерії оцінювання роботи студента протягом семестру.

Задовільно, D, E (60-74). Мати мінімум знань і умінь. Відпрацювати та захистити всі лабораторні роботи та ІДЗ.

Добре, C (75-89). Знати основні теми дисципліни. Відпрацювати та захистити всі лабораторні роботи та практичні завдання та ІДЗ. *Відмінно, A, B (90-100).* Знати всі теми дисципліни. Відпрацювати та захистити всі лабораторні роботи, практичні завдання, пропущені лекції та ІДЗ. Виконати без зауважень всі практичні знання з класичної криптографії. Підготувати реферати по кожному зі змістовних модулів.

Критерії оцінювання знань та умінь студента на комбінованому іспиті.

Задовільно, D, E (60-74). Показати необхідний мінімум теоретичних знань. Розв'язати задачу.

Добре, C (75-89). Знати головні теми теоретичного матеріалу. Розв'язати задачу.

Відмінно, A, B (90-100). Показати повні знання теоретичного матеріалу. Безпомилково розв'язати задачу.

Шкала оцінювання: національна та ECTS

Сума балів за всі види навчальної діяльності	Оцінка ECTS	Оцінка за національною шкалою	
		для екзамену, курсового проєкту (роботи), практики	для заліку
90 – 100	A	відмінно	зараховано
82-89	B	добре	
74-81	C		
64-73	D	задовільно	
60-63	E		
35-59	FX	незадовільно з можливістю повторного складання	не зараховано з можливістю повторного складання
0-34	F	незадовільно з обов'язковим повторним вивченням дисципліни	не зараховано з обов'язковим повторним вивченням дисципліни

Методичне забезпечення

Базова література

1. Золотарьов В. Захист інформації в телекомунікаційних системах // Інформаційні мережі зв'язку. Ч.4 Технології надання інформаційних послуг: навч. Посібник / Безрук В.М., Корольов В.М., Золотарьов В.А., Боцман П.Д., Костромицький А.І., Астраханцев А.А. Капушта С.О. . – Харків: ХНУРЕ, 2011. – с.324-391.
2. Климаш М.М., Лунтовський А.О. Інформаційна безпека розподілених систем. Монографія.- Львів: Національний університет «Львівська політехніка», 2014.
3. Горбенко І.Д. Захист інформації в інформаційно-телекомунікаційних системах : Навч. посіб. для студ. Ч. 1. Криптографічний захист інформації . – Харків, ХНУРЕ, 2004.
4. Максименко В.Н., Афанасьев В.В., Волков Н.В. Защита информации в сетях сотовой подвижной связи. – М.: Горячая линия – Телеком, 2007.
5. Ємець В., Мельник А., Попович Р. Сучасна криптографія. Основні поняття. – Львів: БАК, 2003.
6. Романец Ю.В., Тимофеев П.А., Шаньгин В.Ф. Защита информации в компьютерных системах и сетях. – М.: Радио и связь, 1999. – 328 с.

Допоміжна література

1. Бузов Г.А., Калинин С.В., Кондратьев А.В. Защита от утечки информации по техническим каналам: Учебное пособие. – М.: Горячая линия-Телеком, 2005.
2. Филин С.А. Информационная безопасность. Учебное пособие. – М., Альфа-Прес, 2006.

3. Тарасюк М.В. Защищенные информационные технологии. Проектирование и применение. – М.: Солон-Пресс, 2004.
4. Кузнецов О. О. , Євсєєв С.П., Король О.Г. Захист інформації в інформаційних системах – Харків: Вид. ХНЕУ, 2010.

Методичні вказівки та література до різних видів занять

1. Методичні вказівки до лабораторних робіт з дисципліни «Захист інформації в телекомунікаційних системах» для студентів напряму «Телекомунікації» спеціальності 8.092402 – Інформаційні мережі зв'язку. Упоряд.: В.А.Золотарьов, А.А. Астраханцев, О.В. Федоров,. – Харків, ХНУРЕ, 2008. – 108 с.
2. Криптологія у прикладах, тестах і задачах: навч. посібник / Т.В. Бабенко, Г.М. Гулак, С.О. Сушко, Л.Я. Фомичова. -Дніпропетровськ.: Національний гірничий університет, 2013. - 318 с.
3. Поляков Н.Л., Тищенко А.В. Математические основы криптографии. Задачи и решения. – М.: Финансовый университет, 2015. – 25 с. 4. Правовий захист інформації. Навчальний посібник. / Н.І.Логінова, Р.Р.Дорожбур – Одеса, Фенікс, 2015 – 264 с.

Інформаційне забезпечення

1. Оригінальне програмне забезпечення