Силабус навчальної дисципліни

Інформаційна безпека інноваційної діяльності

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	Другий (магістерський)
Код і назва спеціальності	172 Телекомунікації та радіотехніка
Тип і назва освітньої програми	ОПП «Інформаційно-мережна інженерія»»
Назва дисципліни	Інформаційна безпека інноваційної діяльності
Кількість ЄКТС кредитів	3
Структура дисципліни (розподіл за видами та годинами навчання)	14 год – 7 лекцій, 16 год – 4 лабораторних заняття, 6 год – 3 консультацій, 54 год – самостійна робота, **вид контролю**: залік
Графік (терміни) вивчення дисципліни	1-й рік, II семестр
Передумови для навчання за дисципліною	Раніше мають бути вивчені дисципліни за першим (бакалаврським) рівнем освіти спеціальності 172 Телекомунікації та радіотехника
Компетентності, знання, вміння, розуміння, якими оволодіє здобувач вищої освіти в процесі навчання	Навчальна дисципліна використовується для формування наступних компетентностей: 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; здійснювати організаційно-адміністративні заходи захисту комерційної таємниці
Якість освітнього процесу	Навчально-методичне та матеріально-технічне ресурсне забезпечення освітньої програми, в рамках якої проводиться вивчення дисципліни, відповідає лицензійним вимогам та акредитаційним умовам провадження освітньої діяльності університету. Здійснюється щорічний мониторінг та перегляд навчальної програми дисципліни у відповідності до вимог та 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.

Опис та зміст дисципліни

Мета вивчення дисципліни - здобуваннязнань, навичок і прийомів роботи з інформацією,що становить комерційну таємницю на інноваційному підприємстві.

Зміст

Змістовний модуль 1. Інформаційні ризики інноваційної діяльності

Тема 1. Інформаційна безпека інноваційної діяльності: суть та основні чинники
Тема 2. Методи та засоби несанкціонованого отримання інформації про інноваційну діяльність підприємства
Тема 3. Інформаційні ризики інноваційної діяльності підприємства

Змістовний модуль 2. Захист інформації на інноваційному підприємстві

Тема 1. Таємна інформація про інноваційну діяльність підприємства
Тема 2. Система захисту інформації на інноваційному підприємстві
Тема 3. Організаційно-адміністративний захист інформації на інноваційному підприємстві
Тема 4.Захист інформації в інфокомунікаційній мережі інноваційного підприємств

Результати навчання здобувача вищої освіти

За результатом вивчення дисципліни студенти повинні:

знати: основні організаційно-адміністративні методи захисту комерційної таємниці; застосування технологій по захисту конфіденційної інформації в телекомунікаціях; можливості використання програмних засобів для обмеження доступу до електронних документів як на локальному ПК так і через інформаційно-комунікаційну мережу.

вміти: забезпечувати конфіденційність особистої та службовоїінформації 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 навики для виявляти загроз інформації; аналізувати інформаційні ризики; здійснювати вибір засобів захисту.

володіти (перелік компетенцій) 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; здійснювати організаційно-адміністративні заходи захисту комерційної таємниці.

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) x 2 = 12….20
Контрольна робота №1	(12…20) = 12…20
Контрольна точка № 1	**24…40**
Лабораторні роботи № 3, 4,	(6….10) x 2 = 12….20
Контрольна робота №1	(12…20) = 12…20
Контрольне завдання	(12…20) = 12...20
Контрольна точка № 2	**36…60**
Разом	**60…100**

Як форма підсумкового контролю для дисципліни ІБІД використовується залік.

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.

Шкала оцінювання: національна та ECTS

Сума балів за всі види навчальної діяльності	Оцінка ECTS	Оцінка за національною шкалою	
		для екзамену, курсового проекту (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.,Капуста С.О. . – Харків:ХНУРЕ,2011. – с. 324-391.

2. Филин С.А. Информационная безопасность. Учебное пособие. – М., Альфа-Прес, 2006.

3. Климаш М.М., Лунтовський А.О. Інформаційна безпека розподілених систем. Монографія.- Львів: Національний університет «Львівська політехніка», 2014.

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. Тарасюк М.В. Защищенные информационные технологии. Проектирование и применение. – М.: Солон-Пресс, 2004.

3. Кузнецов О. О. , Євсеєв 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. Правовий захист інформації. Навчальний посібник. / Н.І.Логінова, Р.Р.Дорожбур – Одеса, Фенікс, 2015 – 264 с.

Інформаційне забезпечення

Оригінальне програмне забезпечення