Силабус навчальної дисципліни

Інформаційна безпека електронного бізнесу

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	Інформаційна безпека електронного бізнесу
Кількість ЄКТС кредитів	3
Структура дисципліни (розподіл за видами та годинами навчання)	22 год – 11 лекцій, 20 год – 5 лабораторних заняття, 6 год – 3 консультацій, 57 год – самостійна робота, **вид контролю**: залік
Графік (терміни) вивчення дисципліни	3-й рік, V семестр
Передумови для навчання за дисципліною	Базові знання з дисциплін: інформаційні системи електронної комерції, захист інформації в ТКС, електронні платіжні системи
Компетентності, знання, вміння, розуміння, якими оволодіє здобувач вищої освіти в процесі навчання	Навчальна дисципліна використовується для формування наступних компетентностей: навички по забезпечуванню інформаційної безпеки електронного бізнесу.
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 моніторінг 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 – є здобування знань, навичок і прийомів роботи з програмними та апаратними засобами захисту інформації в електронному бізнесі, такими як криптографічні пакети, програмно-апаратні комплекси мережного захисту, антивірусне програмне забезпечення та інше; здобування спеціальних знань та практичних навичок у використанні сучасних інфокомунікаційних систем електронного бізнесу технологій у професійній діяльності.

Зміст

Змістовний модуль 1 Парадигма інформаційної безпеки електронного бізнесу

Тема 1. Нормативно-правова база захисту інформації в електронному бізнесі
Тема 2. Протоколи автентифікації
Тема 3. Проблеми забезпечення конфіденційності та автентичності інформації в електронному бізнесі
Тема 4. Спеціальні схеми цифрового підпису

Змістовний модуль 2. Захист інформації в системах електронних платежів

Тема 1. Неанонімні СЕП, що працюють в реальному режимі часу
Тема 2. Неанонімні автономні СЕП
Тема 3. Анонімні СЕП, що працюють в реальному масштабі часу
Тема 4. Анонімні автономні СЕП

Змістовний модуль 3 Криптографічні протоколи в електронній комерції

Тема 1. Основні задачі захисту інформації в електронній комерції.
Тема 2. Захищені канали передачі інформації в ЕК
Тема 3. Чесний обмін цифровими підписами та його додатки
Тема 4. Багатосторонні транзакції, комерційні угоди, правові відносини

Результати навчання здобувача вищої освіти

За результатом вивчення дисципліни студенти повинні:

знати: складові криптографічних систем електронних платежів, криптографічні протоколи, які використовуються в сфері електронної комерції та бізнесу; загальні вимоги до організації захищених платіжних систем; криптографічні протоколи розподілення криптографічних ключів, які використовуються в електронному бізнесі.

вміти: досліджувати інфраструктуру криптосистем, включаючи процедури управління криптографічними ключами; користуватися

нормативно-правовою базою у галузі інформаційної безпеки електронного бізнесу; впроваджувати і використовувати обрані заходи забезпечення інформаційної безпеки; використовувати свої теоретичні знання та практичні навики для виявляти загроз інформації в електронному бізнесі; аналізувати інформаційні ризики електронному бізнесу; здійснювати вибір засобів захисту.

володіти (перелік компетенцій) в процесі практичної діяльності в галузі інфокомунікацій навичками по забезпечуванню інформаційної безпеки електронного бізнесу.

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) х 2 = 12….20
Контрольна робота №1	(6…10) = 6…10
Контрольна робота №2	(6…10) = 6…10
Контрольна точка № 1	**24…40**
Лабораторні роботи № 3, 4,5	(6….10)х3 = 18….30
Контрольна робота № 3	(6…10) = 6…10
Контрольна робота №4	(6…10) = 6…10
Контрольна точка № 2	**30…50**
Індивідуальне домашнє завдання	6…10
Разом	**60…100**

Як форма підсумкового контролю для дисципліни використовується залік, під час якого відбувається захист індивідуального домашнього завдання.

Якісні критерії оцінювання в національній шкалі та ECTS

Задовільно, D, E (60-74). Показати необхідний мінімум теоретичних знань. Знати шляхи та методи рішення практичного завдання та вміти використовувати їх на практиці.

Добре, C (75-89). Твердо знати мінімум теоретичних знань. Показати вміння розв’язувати практичне завдання та обґрунтовувати всі етапи запропонованого рішення.

Відмінно, A, B (90-100). Показати повні знання основного та додаткового теоретичного матеріалу. Безпомилково розв'язати практичне завдання, пояснити та обґрунтувати обраний метод розв'язання.

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. Запечкин С.В. Криптографические протоколы и их применение в финансовой и коммерческой деятельности. – М., Горячая линияТелеком, 2007.- 320 с.
2. 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.
3. Климаш М.М., Лунтовський А.О. Інформаційна безпека розподілених систем. Монографія.- Львів: Національний університет «Львівська політехніка», 2014. – 480 с.
4. Горбенко І.Д. Захист інформації в інформаційно-телекомунікаційних системах : Навч. посіб. для студ. Ч. 1. Криптографічний захист інформації . – Харків, ХНУРЕ,2004.

Допоміжна література

1. CUA-14-01A Рекомендації CERT-UA для усунення вразливостей, пов'язаних з некоректним налаштуванням DNSсерверів. – К., ДСТЗІ, 2014. – 12 с.
2. CUA-14-02A Рекомендації CERT-UA для усунення вразливостей, пов'язаних з використанням протоколу SNMP. - К., ДСТЗІ, 2014. – 10 с.

3. CUA-14-03A Рекомендації CERT-UA для усунення вразливостей, пов'язаних з використанням протоколу SSDP. - К., ДСТЗІ, 2014. – 10 с.
4. CUA-14-04A Рекомендації CERT-UA для усунення вразливостей, пов'язаних з використанням протоколу NetBIOS. - К., ДСТЗІ, 2014. – 10 с.
5. CUA-14-05A Рекомендації CERT-UA для усунення вразливостей, пов'язаних з некоректним налаштуванням NTPсерверів/ - К., ДСТЗІ, 2014. – 8 с.
6. CUA-15-01M Опис шкідливого програмного забезпечення Regin. - К., ДСТЗІ, 2015. – 13 с.
7. CUA-15-04R Рекомендації CERT-UA з протидії загрозі інсайдера. - К., ДСТЗІ, 2015. – 13 с.
8. CUA-15-05R БЕЗПЕКА ПОШТОВОГО СЕРВІСУ. - К., ДСТЗІ, 2015. – 9 с.

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

Інформаційне забезпечення
1. Оригінальне програмне забезпечення