ЧЕРКАСЬКИЙ ДЕРЖАВНИЙ БІЗНЕС-КОЛЕДЖ

Кафедра комп'ютерної інженерії та інформаційних технологій

СИЛАБУС

Базова інформація про дисципліну	
Назва дисципліни	СЕ126 Комп'ютерна криптографія / Computer cryptography
Рівень вищої освіти	Перший (бакалаврський)
Галузь знань	12 Інформаційні технології
Спеціальність	123 „Комп'ютерна інженерія"
Освітня програма	Комп'ютерна інженерія
Семестр	2 семестр
Курс	1 курс (за скороченою формою навчання)
Анотація курсу	Навчальна дисципліна спрямована на формування уявлення про принципи шифрування та розшифрування інформації з метою забезпечення конфіденційності, цілісності та доступності даних в інформаційних системах. Основна мета цієї дисципліни – надати студентам глибоке розуміння теоретичних та практичних аспектів криптографічного захисту інформації в електронних системах.
Сторінка курсу в MOODLE	http://78.137.2.119:2929/course/view.php?id=244
Мова викладання	українська
Лектор курсу	Захарова Марія В'ячеславівна, к.т.н., доцент Канали комунікації: СДН «Moodle»: повідомлення в чаті E-mail: lecturer2020student@gmail.com
Місце дисципліни в освітній програмі	
Освітня програма	http://csbc.edu.ua/documents/otdel/oop_kb1.pdf
Перелік загальних компетентностей (ЗК)	Z2. Здатність вчитися і оволодівати сучасними знаннями. Z3. Здатність застосовувати знання у практичних ситуаціях.

Перелік спеціальних компетентностей (СК)	Р4. Здатність забезпечувати захист інформації в комп'ютерних системах та мережах з метою реалізації встановленої політики інформаційної безпеки. Р9. Здатність системно адмініструвати, використовувати, адаптувати та експлуатувати наявні інформаційні технології та системи. Р11. Здатність оформляти отримані робочі результати у вигляді презентацій, науковотехнічних звітів.
Перелік програмних результатів навчання	N6. Вміти застосовувати знання для формулювання і розв'язування технічних задач спеціальності, використовуючи методи, що є найбільш придатними для досягнення поставлених цілей. N9. Вміти застосовувати знання технічних характеристик, конструктивних особливостей, призначення і правил експлуатації апаратних та програмних засобів комп'ютерної інженерії для вирішення технічних задач у професійній діяльності.
	Опис дисципліни
Структура навантаження на студента	Загальна кількість годин – 90 Кількість кредитів – 3 Кількість лекційних годин – 15 Кількість практичних занять – 30 Кількість годин для самостійної роботи студентів – 45 Форма підсумкового контролю – екзамен
Методи навчання	Словесні (лекції, пояснення), наочні (демонстрація матеріалів), інструктивний, репродуктивний, частково-пошуковий, тренувальний, пояснювально-демонстраційний, проблемно-орієнтоване навчання.
	Зміст дисципліни
Тема 1. Задачі криптографії. Основні поняття та положення комп'ютерної криптографії	Основні поняття та положення комп'ютерної криптографії. Принципи криптографічного захисту інформації/ Класифікація шифрів.

Тема 2. Класичні та сучасні симетричні криптосистеми.	Шифри перестановки та простої заміни. Шифр Цезаря з ключовим словом. Біграмний шифр Плейфейра. Шифр Віженера. Алгоритм DES. Режими його роботи. Шифрування алгоритмом IDEA.
Тема 3. Системи з відкритим ключем або асиметричні криптосистеми.	Арифметика асиметричних криптосистем. Генерація ключів. Криптосистема RSA. Шифрування та дешфрування. Шифрування та дешифрування в криптосистемі Ель–Гамаля. Ефективність та надійність криптосистем.
Тема 4. Алгоритми електронного цифрового підпису.	Поняття електронного цифрового підпису. Електронний цифровий підпис в системах RSA та Ель– Гамаля. Алгоритм DSA. Достовірність, конфіденційність підписів у різних алгоритмах.
Теми 5. Криптографічні протоколи.	Поняття криптографічного протоколу. Протоколи обміну ключем, розподілу.
Тема 6. Керування криптографічними ключами.	Види та стадії життєвого циклу ключів. Розподіл крипторгафічних ключів. Алгоритм Діффі-Хеллмана. Збереження ключів. Термін дії ключів.
Тема 7. Методи криптоаналізу	Поняття криптоаналізу. Частотний аналіз. Метод зустрічі посередині. Алгоритми класичного криптоаналізу.
Політика дисципліни	
Політика відвідування	Регулярне відвідування всіх видів занять, своєчасність виконання самостійної роботи. За об'єктивних причин (наприклад, хвороба, міжнародне стажування) навчання зорганізується в он-лайн формі за погодженням із керівником курсу.
Політика щодо дедлайнів та перескладання	Роботи, які здаються із порушенням термінів без поважних причин, оцінюються на нижчу оцінку.
Академічна доброчесність	У випадку недотримання політики академічної доброчесності (плагіат, самоплагіат, фабрикація, фальсифікація, списування, обман, хабарництво) передбачено повторне проходження оцінювання.

Система оцінювання

Поточний контроль здійснюється протягом семестру під час проведення практичних, семінарських та інших видів занять і оцінюється сумою набраних балів (максимальна сума – 100 балів; мінімальна сума, що дозволяє студенту отримати атестацію з предмету – 60 балів); підсумковий/ семестровий контроль, проводиться у формі іспиту, відповідно до графіку навчального процесу.
Підсумкова оцінка за умови іспиту виставляється як загальна сума балів набраних за результатами поточного (70%) та підсумкового контролю

Накопичування рейтингових балів з навчальної дисципліни (екзамен)

Види навчальної роботи	**Мах кількість балів**
Виконання практичних робіт № 1,2,3,4 по 5 балів	20
Виконання практичних робіт № 5,6,7,8 по 5 балів	20
Індивідуальні завдання	30
Завдання екзамену	30
Разом	100

Шкала оцінювання

ECTS	**Бали**	**Зміст**
A	90-100	Бездоганна підготовка в широкому контексті
B	80-89	Повні знання, міцні вміння
C	70-79	Хороші знання та вміння
D	65-69	Задовільні знання, стереотипні вміння
E	60-64	Виконання мінімальних вимог діяльності в стандартних умовах
FX	35-59	Слабкі знання, відсутність умінь
F	1-34	Необхідний повторний курс

Список рекомендованих джерел

Основна

1. Гапак О.М. Основи криптоаналізу. Криптографічні протоколи: навчальний посібник для студентів напряму підготовки «комп'ютерна інженерія». – Ужгород: «АУТДОР-ШАРК», 2021. – 120 с.
2. Горбенко Ю.І. Побудування та аналіз систем, протоколів і засобів криптографічного захисту інформації: монографія/ За заг. ред. д.т.н., професора Горбенка І.Д. – Харків: Вид. «Форт», 2015.
3. Методи і алгоритми захисту інформаційних ресурсів комп'ютерних систем: навчальний посібник / В. М. Джулій, Ю. П. Кльоц, І. В. Муляр, В. М. Чешун. – Хмельницький: ХмНУ, 2020. – 196 с.
4. Інформаційна безпека держави: навчальний посібник/ В.І. Гур'єв, Д.Б. Мехед, Ю.М. Ткач, І.В. Фірсова. – Ніжин: ФОП Лук'яненко В.В. ТПК «Орхідея», 2018. – 166 с.
5. Cyber Security for Cyber Physical Systems / Saqib Ali, Taiseera Al Balushi, Zia Nadir, Omar Khadeer Hussain. – Cham, Switzerland : Springer, 2018. – 174 p.
6. Хорошко В. О. Проєктування комплексних систем захисту інформації. Підручник / В. О. Хорошко, І. М. Павлов, Ю. Я. Бобало, В. Б. Дудикевич, І. Р. Опірський, Л. Т. Пархуць. Львів : Видавництво Львівської політехніки, 2020. 320 с.

Додаткова

1. Грищук Р.В. Основи кібернетичної безпеки: Монографія / Р.В. Грищук, Ю.Г. Даник; ред. Ю.Г. Данника. – Житомир: ЖНАЕУ, 2016. 636 с.
2. Коженевський С.Р. Термінологічний довідник з питань захисту інформації / С.Р. Коженевський, Г.В. Кузнецов, В.О. Хорошко, Д.В. Чирков. – К.: ДУІКТ, 2007. – 382 с.
3. Корченко А. О. Банківська безпека. / А. О. Корченко, Л. М. Скачек, В. О. Хорошко. – К. : ПВП «Задруга». – 2014. – 185 с.
4. Ластівка Г. І. Технічний захист інформації в інформаційних та телекомунікаційних системах: Навчальний посібник / Г. І. Ластівка, П. М. Шпатар – Чернівці: Чернівецький національний університет, 2018. - 252 с.
5. Методика та організація наукових досліджень: Навч. посіб. / С.Е. Важинський, Т І. Щербак. – Суми: СумДПУ імені А. С. Макаренка, 2016. – 260 с.
6. Надійність, контроль комп'ютерних систем та мереж [Текст]: конспект лекцій для студентів спеціальності 123 – «Комп'ютерна інженерія » денної та заочної форм навчання / уклад. О.І. Міскевич, К.Я.Бортник. – Луцьк: Луцький НТУ, 2017. – 44 с.
7. Нормування показників надійності технічних засобів : навчальний посібник / О. М. Василевський, О. Г. Ігнатенко. – Вінниця : ВНТУ, 2013. – 160 с.
8. Рибальський О.В. Основи інформаційної безпеки. Підручник для курсантів ВНЗ МВС України / Рибальський О.В., Смаглюк В.М., Хахановський В.Г. – К.: НАВС, 2013. – 255 с.
9. Тарнавський Ю. А. Технології захисту інформації: підручник / Ю.А. Тарнавський. – Київ: КПІ ім. Ігоря Сікорського, 2018. – 162 с.
10. Федун І. В. Основи теорії надійності та контролю якості виробів електронної техніки: Лабораторний практикум. – Вінниця: ВДТУ, 2003. – 71 с.

11. Security and Privacy inInternet of Things (IoTs): Models, Algorithms, and Implementations / Edited by Fei Hu. – Taylor & Francis Group, 2016. – 564 p.