ЧЕРКАСЬКИЙ ДЕРЖАВНИЙ БІЗНЕС-КОЛЕДЖ

Кафедра комп'ютерної інженерії та інформаційних технологій

СИЛАБУС

Базова інформація про дисципліну	
Назва дисципліни	**ОК15/Цифрова безпека/Digital Security**
Рівень вищої освіти / фахової передвищої освіти	Фахова передвища
Галузь знань	07 «Управління та адміністрування»
Спеціальність	072 Фінанси, банківська справа, страхування та фондовий ринок
Освітня програма	Фінанси, банківська справа та страхування
Семестр	4 семестр
Факультет / відділення	Відділення підприємництва та маркетингу Відділення економіки, обліку та фінансів
Курс	2 курс (9 кл.)
Анотація курсу	Навчальна дисципліна зосереджена на вивченні складових цифрової безпеки та захисту інформації, а також їх класифікацій та характеристик. В процесі вивчення курсу студенти ознайомлюються з сучасними програмно-технічними засобами забезпечення цифрової безпеки; навчаться виявляти основні загрози цифрової безпеки, аналізувати і використовувати типові криптографічні засоби та методи захисту інформації, у тому числі електронний цифровий підпис, антивірусний захист.
Сторінка курсу в MOODLE	http://78.137.2.119:2929/course/view.php?id=791
Мова викладання	українська
Лектор курсу	Бреус Р.В., викладач канали комунікації: СДН «Moodle»: повідомлення в чаті E-mail: breus.roksolana@gmail.com
Місце дисципліни в освітній програмі	
Освітня програма	Фінанси, банківська справа, страхування та фондовий ринок
Перелік загальних компетентностей (ЗК)	ЗК 05. Знання і розуміння предметної області та розуміння професійної діяльності. ЗК 06. Здатність застосовувати знання у практичних ситуаціях. ЗК 07. Здатність використовувати інформаційні та комунікаційні технології.

	ЗК 08. Здатність до пошуку, оброблення та аналізу інформації з різних джерел.
Перелік спеціальних компетентностей (СК)	-
Перелік програмних результатів навчання	**РН 07.** Застосовувати сучасне інформаційне та програмне забезпечення для отримання й обробки даних у сфері фінансів, банківської справи та страхування. **РН 08.** Здійснювати пошук, відбір та опрацювання інформації з різних джерел у процесі професійної діяльності. **РН 15.** Виявляти навички самостійної роботи та роботи в команді, демонструвати гнучке мислення, відкритість до нових знань
Опис дисципліни	
Структура навантаження на студента	Загальна кількість годин – 90 Кількість кредитів – 3 Кількість лекційних годин – 14 Кількість практичних занять – 16 Кількість годин для самостійної роботи студентів – 60 Форма підсумкового контролю – залік
Методи навчання	Розповідь, Пояснення, Бесіда, Інструктаж, Дискусія, Практична робота, Пробні вправи, Творчі вправи, Усні вправи, Практичні вправи
Зміст дисципліни	
Тема 1. Вступ до дисципліни цифрова безпека.	Вступ до цифрової безпеки. Основні загрози цифровій безпеці. Принципи безпеки в цифровому середовищі. Інструменти та методи захисту. Безпека в Інтернеті та соціальних мережах. Безпека мобільних пристроїв.
Тема 2. Основні загрози для безпеки інформації та способи їхнього подолання.	Основні поняття та визначення. Типи загроз безпеки інформації. Класифікація загроз за методами впливу. Шкідливі програми та їх види. Загрози через людський фактор. Загрози для конфіденційності, цілісності та доступності інформації. Захист від загроз безпеки інформації.
Тема 3. Методи аутентифікації та управління доступом до інформаційних систем.	Основні поняття та визначення. Основні методи аутентифікації. Типи управління доступом. Принципи мінімальних привілеїв та необхідного доступу. Технології аутентифікації та управління доступом.
Тема 4. Особливості безпечного зберігання даних.	Основні поняття та визначення. Методи зберігання даних. Шифрування даних як метод захисту. Контроль доступу до даних. Резервне копіювання даних. Захист даних від фізичних загроз. Використання технологій для захисту

	даних. Використання технологій для захисту даних.
Тема 5. Забезпечення безпеки в комп'ютерних мережах.	Основні поняття та визначення. Типи загроз в мережах. Механізми захисту мереж. Шифрування та захист передавання даних. Контроль доступу в мережах. Безпека в бездротових мережах.
Тема 6. Соціальна інженерія та правила безпечного використання соціальних мереж.	Основні поняття та визначення. Методи соціальної інженерії. Методи захисту від соціальної інженерії. Правила безпечного використання соціальних мереж. Основи безпеки при публікаціях у соціальних мережах. Ризики використання соціальних мереж для компаній та організацій. Інструменти та технології для захисту у соціальних мережах.
Тема 7. Безпека програмного забезпечення та резервне копіювання і відновлення даних.	Основні поняття та визначення. Основи безпеки програмного забезпечення. Резервне копіювання даних. Відновлення даних. Інтеграція безпеки програмного забезпечення та резервного копіювання. Управління ризиками та найкращі практики.
Тема 8. Нові напрямки в галузі цифрової безпеки.	Основні поняття та визначення. Інтеграція штучного інтелекту та машинного навчання. Захист даних у хмарних середовищах. Загроза кіберзлочинності та нові види атак. Біометрична аутентифікація та багатофакторна аутентифікація. Захист персональних даних та відповідність регламентам (GDPR, CCPA). Інтернет речей (IoT) та його безпека.
Політика дисципліни	
Політика відвідування	Регулярне відвідування всіх видів занять, своєчасність виконання самостійної роботи. За об'єктивних причин (наприклад, хвороба, міжнародне стажування) навчання організується 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 заліку, відповідно до графіку навчального процесу. Підсумкова оцінка заліку виставляється як загальна сума балів набраних за результатами поточного контролю.

Накопичування рейтингових балів з навчальної дисципліни

Види навчальної роботи	Мах кількість балів
Аудиторна	
Практичні завдання (4 пр по 10 балів – 6 балів за роботу та 4 бали за заключний тест з практичного заняття)	40
Модульні контрольні роботи (2 роботи по 10 балів)	20
Тестування (2 тестування по 10 балів)	20
Індивідуальне завдання	20

Список рекомендованих джерел

Основна

1. Полторак В. П., Савчук О. В. Інформаційна безпека та захист даних в комп'ютерних технологіях і мережах. Вибрані розділи: навч. посіб. Київ: КПІ ім. Ігоря Сікорського, 2021. 384 с. URL: https://ela.kpi.ua/handle/123456789/47380
2. Тарнавський Ю. А. Безпека інформаційних систем: підручник для студ. спеціальності 122 «Комп'ютерні науки», освітня програма «Цифрові технології в енергетиці». Київ: КПІ ім. Ігоря Сікорського, 2023. 163 с. URL: https://ela.kpi.ua/handle/123456789/62709
3. Титова Н. М., Рідей Н. М., Настрадін В. П., Присяжнюк М. М., Мамченко С. М., Артюх С. В., Яворська Р. О. Інформаційна безпека та кібербезпека держави: навч. посіб. Київ: Ліра-К, 2024. 224 с.
4. Адміністрація Держспецзв'язку. Методичні рекомендації щодо підвищення рівня кіберзахисту систем електронного документообігу: наказ від 30.08.2023 № 773. URL: https://zakon.rada.gov.ua/go/v0773519-23
5. Державна служба спеціального зв'язку та захисту інформації України. Методичні рекомендації щодо підвищення рівня кіберзахисту систем електронного документообігу. 2023. URL: https://cybersec.net.ua/normatyvni-dokumenty/591-metodychni-rekomendatsii-shchodo-pidvyshchennia-rivnia-kiberzakhystu-system-elektronnoho-dokumentoobihu-vid-derzhspetszviazku.html

Додаткова

1. Соловйов В. М., Кузнєцов С. Д. Кібербезпека: основи захисту інформації в інформаційно-комунікаційних системах: навч. посіб. Київ: Національний авіаційний університет, 2020. 256 с.
2. Гнатюк С. М., Коваленко А. О. Основи кібербезпеки: навч. посіб. Київ: Вид-во НТУУ «КПІ ім. Ігоря Сікорського», 2019. 312 с.
3. Петренко О. В., Іванов І. І. Захист інформації в комп'ютерних системах: підручник. Харків: ХНУРЕ, 2021. 348 с.

4. Сидоренко В. В., Мельник М. М. Кібербезпека та захист інформації: навч. посіб. Львів: Львівська політехніка, 2022. 290 с.
5. Кравченко П. П., Литвиненко О. О. Інформаційна безпека: сучасні аспекти та технології: монографія. Одеса: ОНПУ, 2020. 275 с.
6. Дерев’янко Б. В., Шевченко О. В. Кіберзахист критичної інфраструктури: метод. рекомендації. Київ: Держспецзв’язку, 2021. 88 с.
7. Морозов А. В., Кузьменко О. С. Технології забезпечення інформаційної безпеки: навч. посіб. Дніпро: ДНУ ім. Олеся Гончара, 2019. 234 с.
8. Федоренко В. Г., Соколовський С. В. Кібербезпека: теорія та практика: підручник. Київ: КНЕУ, 2023. 320 с.
9. Литвиненко В. В., Гончарук С. М. Основи інформаційної безпеки: навч. посіб. Харків: ХНУ ім. В. Н. Каразіна, 2021. 298 с.
10. Бондаренко С. В., Ковальчук О. П. Кібербезпека в державному управлінні: монографія. Київ: НАДУ, 2022. 310 с.