ЧЕРКАСЬКИЙ ДЕРЖАВНИЙ БІЗНЕС-КОЛЕДЖ

СИЛАБУС

Базова інформація про дисципліну	
Назва дисципліни	CE029 Цифрова безпека / Digital security
Рівень вищої освіти	Перший (бакалаврський)
Семестр	2 семестр
Анотація курсу	Навчальна дисципліна спрямована вивчення основної концепції цифрової безпеки, на формування уявлення про загрози безпеки інформації, механізми авторизації, аутентифікації та управління доступом; принципів безпеки віртуальних локальних мереж та безпечного зберігання даних та використання соціальних мереж; систем резервного копіювання та відновлення даних.
Сторінка курсу в MOODLE	http://78.137.2.119:2929/course/view.php?id=659
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	
Перелік загальних компетентностей (ЗК)	ЗК 04. Здатність до пошуку, оброблення та аналізу інформації з різних джерел. ЗК 05 Здатність працювати в команді.
Перелік спеціальних компетентностей (СК)	ФК 07. Здатність використовувати сучасне програмне забезпечення для створення об'єктів дизайну.
Перелік програмних результатів навчання	ПРН 01. Застосовувати набуті знання і розуміння предметної області та сфери професійної діяльності у практичних ситуаціях. ПРН 05. Розуміти і сумлінно виконувати свою частину роботи в команді; визначати пріоритети професійної діяльності.

	ПРН 06. Усвідомлювати відповідальність за якість виконуваних робіт, забезпечувати виконання завдання на високому професійному рівні. ПРН 17. Застосовувати сучасне загальне та спеціалізоване програмне забезпечення у професійній діяльності (за спеціалізаціями).
Опис дисципліни	
Структура навантаження на студента	Загальна кількість годин – 120 Кількість лекційних годин – 45 Кількість практичних занять – 45 Кількість кредитів – 3 Кількість годин для самостійної роботи студентів – 75 Форма підсумкового контролю – залік
Методи навчання	Словесні (інформаційна, самостійна робота з джерелами інформації, науково-популярна розповідь); Наочні (презентаційні повідомлення) Практичні (лабораторні роботи); Інтерактивні методи (дистанційні консультації).
Зміст дисципліни	
Тема 1. Вступ до цифрової безпеки	Основні поняття терміни і концепції цифрової безпеки. Заходи України із забезпечення безпеки національної інфосфери та протидії проявам кіберзлочинності. Взаємозв'язок інформаційного та кіберпросторів.
Тема 2. Загрози безпеки інформації.	Види загроз: віруси, трояни, шкідливе програмне забезпечення. Фішинг та соціальна інженерія. Наслідки атак на особисті та професійні дані користувача.
Тема 3. Аутентифікація та управління доступом.	Методи аутентифікації користувача. Біометрична аутертифікація. Багатофакторна аутентифікація. Політика безпеки. Управління ролями та доступом.

Тема 4. Безпечне зберігання даних.	Основні методи шифрування (симетричне, асиметричне). Використання криптографії в дизайні. Резервне копіювання: локальні та хмарні рішення. Небезпеки незахищеного зберігання.
Тема 5. Безпека в мережах.	Основи безпеки Wi-Fi. VPN та їх значення. Безпечний обмін даними в Інтернеті.
Тема 6. Соціальна інженерія.	Визначення соціальної інженерії. Приклади маніпуляцій та їх наслідки. Як захиститися від соціальної інженерії.
Тема 7. Правила безпечного використання соціальних мереж.	Конфіденційність в соціальних мережах. Приватність профілю. Вплив соціальних мереж на репутацію дизайнера.
Тема 8. Безпека програмного забезпечення	Категорії програмного забезпечення. Вибір надійних програм для дизайну. Вирішення проблем безпеки в ПЗ.
Тема 9. Резервне копіювання та відновлення даних.	Важливість резервного копіювання. Стратегії резервного копіювання. Процеси відновлення даних.
Тема 10. Правові аспекти цифрової безпеки.	Основи законодавства про захист даних. Авторське право та використання чужих матеріалів. Поведінка користувачів та їх вплив на безпеку. Як зменшити ризики людського фактору.
Тема 11. Оцінка ризиків у цифровій безпеці.	Методології оцінки ризиків. Як виявити вразливості в проектах. Розробка плану реагування на інциденти.
Тема 12. Тренди у цифровій безпеці.	Новітні технології та рішення для безпеки. Вплив штучного інтелекту на безпеку.
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 заліку, відповідно до графіку навчального процесу.
Підсумкова оцінка за умови заліку виставляється як загальна сума балів, набраних за результатами поточного контролю.

Накопичування рейтингових балів з навчальної дисципліни (залік)

Види навчальної роботи	**Мах кількість балів**
Виконання практичних робіт № 1,2,3,5,6 по 5 балів	30
Виконання практичних робіт № 7,8 по 10 балів	20
Модульні контрольні роботи (2 к.р.)	20
Презентація	15
Індивідуальні практичні завдання	15
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. Бурячок В. Л. Інформаційний та кіберпростори: проблеми безпеки, методи та засоби боротьби : підручник / В. Л. Бурячок, Г. М. Гулак, В. Б. Толубкл. – Львів : Магнолія, 2020. – 448 с.
2. 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.
3. Хорошко В. О.М. 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. Корченко А. О. Банківська безпека. / А. О. Корченко, Л. М. Скачек, В. О. Хорошко. – К. : ПВП «Задруга». – 2014. – 185 с.
3. 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.
4. Методика та організація наукових досліджень: Навч. посіб. / С.Е. Важинський, Т І. Щербак. – Суми: СумДПУ імені А. С. Макаренка, 2016. – 260 с.
5. 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.
6. Тарнавський Ю. А. Технології захисту інформації: підручник / Ю.А. Тарнавський. – Київ: КПІ ім. Ігоря Сікорського, 2018. – 162 с.
7. Федун І. В. Основи теорії надійності та контролю якості виробів електронної техніки: Лабораторний практикум. – Вінниця: ВДТУ, 2003. – 71 с.
8. Security and Privacy inInternet of Things (IoTs): Models, Algorithms, and Implementations / Edited by Fei Hu. – Taylor & Francis Group, 2016. – 564 p.