ЧЕРКАСЬКИЙ ДЕРЖАВНИЙ БІЗНЕС-КОЛЕДЖ

СИЛАБУС

Базова інформація про дисципліну	
Назва дисципліни	Кібербезпека
Рівень вищої освіти	Перший (бакалаврський)
Семестр	ІІ семестр
Кафедра/циклова комісія	Кафедра комп'ютерної інженерії та інформаційних технологій
Анотація курсу	Навчальна дисципліна спрямована вивчення основної концепції кібербезпеки, на формування уявлення про методи моніторингу, виявлення, аналізу і нейтралізації кібератак, забезпечення захисту інформаційних ресурсів, комплекс вимог до системи забезпечення кібербезпеки, стандарти кібербезпеки; механізми авторизації, аутентифікації та акаунтінгу; принципів безпеки віртуальних локальних мереж; систем виявлення атак та запобігання вторгненням.
Сторінка курсу в MOODLE	http://78.137.2.119:1919/m72/course/view.php?id=1024
Мова викладання	українська
Лектор курсу	Заболотній Сергій Васильович, професор канали комунікації: СДН «Moodle»: повідомлення в чаті E-mail: zabolotnii.serhii@csbc.edu.ua
Місце дисципліни в освітній програмі	
Перелік загальних компетентностей (ЗК)	Здатність вчитися і оволодівати сучасними знаннями. Знання та розуміння предметної області та розуміння професійної діяльності. Здатність застосовувати знання у практичних ситуаціях. Здатність працювати з інформацією, у тому числі у глобальних комп'ютерних мережах.
Перелік спеціальних компетентностей (СК)	Здатність забезпечувати захист інформації в комп'ютерних системах та мережах з метою реалізації встановленої політики інформаційної безпеки. Здатність системно адмініструвати, використовувати, адаптувати та експлуатувати наявні інформаційні

	технології та системи. Здатність оформляти отримані робочі результати у вигляді презентацій, науковотехнічних звітів.
Перелік програмних результатів навчання	Вміти застосовувати знання для формулювання і розв'язування технічних задач спеціальності, використовуючи методи, що є найбільш придатними для досягнення поставлених цілей. 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 – 17 Кількість практичних занять – 34 Кількість годин для самостійної роботи студентів – 39 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. Кіберпростір, кібербезпека та кібертероризм.	Кіберпростір і кібербезпека – головні ознаки нової інформаційної цивілізації. Заходи України із забезпечення кібербезпеки національної інфосфери та протидії проявам кіберзлочинності. Взаємозв'язок інформаційного та кіберпросторів.
Тема 2. Методи забезпечення кібербезреки.	Основні методи забезпечення інформаційної безпеки. Складові кібернетичної безпеки. Головні проблеми забезпечення кібернетичної безпеки, їх причини.
Тема 3. Міжнародний досвід організації кібербезпеки	Проблеми забезпечення кібербезпеки на міжнородному рівні. Провідні компанії з кібербезпеки. Ситуація в Україні.

	Процедура ефективного варіанта реагування на кібернетичні втручання і загрози.
Тема 4. Інциденти у сфері високих технологій: характерні ознаки та проблемні аспекти.	Класифікація джерел інцидентів, а також способів, об'єктів та результатів їхнього впливу. Процес управління інцидентами ІБ. Пріорітети забезречення кібербезпеки.
Тема 5. Особливості кібероборони держави	Основні завдання кібероборони. Стратегічні цілі системи кібероборони, її проектування.
Тема 6. Технологічні аспекти забезпечення кібербезпеки інформаційних ресурсів	Основні технологічні аспекти захисту в інформаційних системах. Особливості систем виявлення кіберзагроз. Оцінка кіберризиків.
Тема 7. Управління кібербезпекою.	Характеристика завдань управління кібербезпекою. Принципи управління кібербезпекою. Інструментарій.
Тема 8. Практичні аспекти забезпечення кібербезпеки.	Кібернавчання.Призначення, склад, підготовка. Сутність та можливості дій у кіберпросторі. Сучасні підходи до оцінки ризиків інформаційних систем. Класифікація кіберзброї. Базові принципи кіберзахисту.
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 або іспиту, відповідно до графіку навчального процесу.

Підсумкова оцінка за умови заліку виставляється як загальна сума балів, набраних за результатами поточного контролю.

Підсумкова оцінка за умови іспиту виставляється як загальна сума балів набраних за результатами поточного (70%) та підсумкового 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

1. Безопастность информационных систем. Кияев В.И., Граничин О.Н. Национальный Открытый Университет “ИНТУИТ”: 2016. - 192 с.
2. Даник Ю.Г. Основи кібербезпеки та кібероборони: підручник / Ю.Г. Даник, П.П. Воробієнко, В.М. Чернега. – Одеса.: ОНАЗ ім. О.С. Попова, 2019. − 320 с.
3. Грищук Р.В. Основи кібернетичної безпеки: Монографія / Р.В. Грищук, Ю.Г. Даник; ред. Ю.Г. Данника. – Житомир: ЖНАЕУ, 2016. 636 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. 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.
6. Корченко А. О. Банківська безпека. / А. О. Корченко, Л. М. Скачек, В. О. Хорошко. – К. : ПВП «Задруга». – 2014. – 185 с.
7. 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.
8. 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.
9. Методика та організація наукових досліджень: Навч. посіб. / С.Е. Важинський, Т І. Щербак. – Суми: СумДПУ імені А. С. Макаренка, 2016. – 260 с.
10. 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.
11. Тарнавський Ю. А. Технології захисту інформації: підручник / Ю.А. Тарнавський. – Київ: КПІ ім. Ігоря Сікорського, 2018. – 162 с.
12. Федун І. В. Основи теорії надійності та контролю якості виробів електронної техніки: Лабораторний практикум. – Вінниця: ВДТУ, 2003. – 71 с.
13. Хорошко В. О.мПроєктування 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.
14. Cyber Security for Cyber Physical Systems / Saqib Ali, Taiseera Al Balushi, Zia Nadir, Omar Khadeer Hussain. – Cham, Switzerland : Springer, 2018. – 174 p.
15. Security and Privacy inInternet of Things (IoTs): Models, Algorithms, and Implementations / Edited by Fei Hu. – Taylor & Francis Group, 2016. – 564 p.