ЧЕРКАСЬКИЙ ДЕРЖАВНИЙ БІЗНЕС-КОЛЕДЖ

Кафедра комп'ютерної інженерії та інформаційних технологій

СИЛАБУС

Базова інформація про дисципліну	
Назва дисципліни	**CE112 / Вступ до Кібербезпеки / Introduction to Cybersecurity**
Рівень вищої освіти / фахової передвищої освіти	Перший (бакалаврський)
Семестр	1
Факультет /відділення	Бакалаврської підготовки
Анотація курсу	Метою навчальної дисципліни є формування у студентів цілісного уявлення про спеціальність кібербезпека та базових знань в даній галузі. Курс надає студентам загальне уявлення про сутність кібербезпеки та її важливість в сучасному цифровому світі. Здобувачі освіти дізнаються про різноманітні види кіберзагроз, включаючи хакерські атаки, віруси, фішинг, витік даних тощо, та здобудуть знання про оцінку ризиків для організацій та окремих осіб. Курс ознайомить з основними принципами та методами захисту інформації, включаючи шифрування, аутентифікацію, авторизацію та інші механізми. Слухачі курсу навчаться виявленню та ліквідації кіберінцидентів. Курс допоможе у дослідженні ролі інструментів моніторингу та спостереження в процесі забезпечення кібербезпеки. Студенти також зможуть застосовувати набуті знання на практичних заняттях, що допоможе закріпити навички.
Сторінка курсу в MOODLE	http://78.137.2.119:2929/course/view.php?id=672
Мова викладання	Українська
Викладач курсу	Викладач Бреус Р.В. канали комунікації: СДН «Moodle»: повідомлення в чаті. E-mail: breus.roksolana@gmail.com

Місце дисципліни в освітній програмі	
Перелік загальних компетентностей (ЗК)	Здатність вчитися і оволодівати сучасними знаннями. Здатність застосовувати знання у практичних ситуаціях. Вміння виявляти, ставити та вирішувати проблеми.
Перелік спеціальних компетентностей (СК)	Здатність застосовувати законодавчу та нормативно-правову базу, а також державні та міжнародні вимоги, практики і стандарти з метою здійснення професійної діяльності в галузі комп'ютерної інженерії. Здатність забезпечувати захист інформації, що обробляється в комп'ютерних та кіберфізичних системах та мережах з метою реалізації встановленої політики інформаційної безпеки.
Перелік програмних результатів навчання	Знати новітні технології в галузі комп'ютерної інженерії. Знати та розуміти вплив технічних рішень в суспільному, економічному, соціальному і екологічному контексті. Вміти поєднувати теорію і практику, а також приймати рішення та виробляти стратегію діяльності для вирішення завдань спеціальності з урахуванням загальнолюдських цінностей, суспільних, державних та виробничих інтересів. Якісно виконувати роботу та досягати поставленої мети з дотриманням вимог професійної етики.

Опис дисципліни	
Структура навантаження на студента	Загальна кількість годин – 180 Кількість кредитів – 6 Кількість лекційних годин – 30 Кількість практичних годин – 30 Кількість годин для самостійної роботи студентів – 120 Форма підсумкового контролю – залік.
Методи навчання	Словесні (лекції, пояснення), наочні (демонстрація матеріалів), інструктивний, репродуктивний, частково-пошуковий, тренувальний, пояснювально-демонстраційний, проблемно-орієнтоване навчання.
Зміст дисципліни	
Тема 1. Основні положення забезпечення кібербезпеки.	Сутність кібербезпеки інформаційного суспільства. Кібербезпека як складова міжнародної, регіональної та національної безпеки.
Тема 2. Сутність кібербезпеки інформаційного суспільства.	Кібербезпека як складова міжнародної, регіональної та національної безпеки. Кіберінциденти: передумови скоєння та наслідки.
Тема 3. Загрози у сфері кібербезпеки.	Зміст, класифікація та ознаки кіберзагроз. Основні характеристики кіберзагроз. Дії у кіберпросторі та їх особливості (Сутність, цілі та задачі кібердій. Класифікація форм і способів кібердій). Система кібердій. Основи кіберрозвідки. Основи кіберзахисту. Основи кібервпливу.
Тема 4. Основи міжнародної співпраці з питань забезпечення кібербезпеки.	Проблеми забезпечення кібербезпеки на міжнародному рівні. Діяльність Міжнародного союзу електрозв’язку щодо забезпечення кібербезпеки. Напрями міжнародного співробітництва з питань забезпечення кібербезпеки.
Тема 5. Напрями забезпечення кібербезпеки України	Основні положення Стратегії кібербезпеки України. Сутність та завдання Національної системи забезпечення кібербезпеки України. Пріоритети та напрями забезпечення кібербезпеки України згідно з чинним законодавством. Основи та особливості кібероборони держави.

Тема 6. Технологічні аспекти забезпечення кібербезпеки інформаційно-телекомунікаційних систем та інформаційних ресурсів	Характеристика основних завдань управління кібербезпекою. Характеристика сучасних кібератак на інформаційно- телекомунікаційні системи та інформаційні ресурси в умовах ведення кібервійни. Сутність та класифікація кібератак на інформаційно- телекомунікаційні системи та інформаційні ресурси. Характеристика APT-кібератак як основної форми боротьби в кіберпросторі.
Тема 7. Технологічні аспекти захисту інформації в інформаційно-телекомунікаційних системах.	Технологічні рішення щодо ідентифікації, автентифікації та авторизації користувачів інформаційно-телекомунікаційної системи. Антивірусний захист інформаційно-телекомунікаційної системи.
Тема 8. Використання брандмауерів (firewall) для контролю та фільтрації трафіка в інформаційно-телекомунікаційних системах	Особливості використання технологій та програмних засобів криптозахисту та криптоаналізу інформації в інформаційно-телекомунікаційних системах. Особливості використання віртуальних захищених мереж (VPN) для забезпечення кібербезпеки інформаційно-телекомунікаційних систем.
Тема 9. Практичні аспекти забезпечення кібербезпеки	Основи організації підготовки фахівців з кібербезпеки. Аналіз досвіду провідних країн світу з підготовки фахівців кібербезпеки.
Тема 10. Загальні характеристики планування та проведення операцій у кіберпросторі та через кіберпростір.	Сутність та можливості дій у кіберпросторі. Сутність та зміст кібероперацій. Підходи щодо планування кібероперацій.
Тема 11. Методика планування операцій, які включають дії в кіберпросторі.	Координація та синхронізація дій у кіберпросторі. Процес прийняття рішень. Розробка варіантів способів дій. Аналіз варіантів способів дій. Порівняння варіантів способів дій. затвердження варіантів способів дій.
Тема 12. Оцінки інформаційних ризиків та управління ними.	Способи оцінки інформаційних ризиків.
Тема 13. Оцінки інформаційних ризиків та управління ними.	Сучасні підходи до оцінки ризиків інформаційних технологій.

Тема 14. Кіберзброя.	Сутність та призначення кіберзброї. Класифікація кіберзброї
Тема 15. Кіберзброя.	Базові принципи побудови кіберзброї.
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 заліку виставляється як загальна сума балів, набраних за результатами поточного контролю.	

Накопичування рейтингових балів з навчальної дисципліни	
Види навчальної роботи	**Мах кількість балів**
Практичні завдання (5 пр.з. по 5 б.)	25
Модульні контрольні роботи (2 по 15 балів)	30
Тестування (2 тестування по 10 б.)	20
Індивідуальне завдання	25
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. Основи кіберпростору, кібербезпеки та кіберзахисту. Навч. посіб. / В. М. Богуш, В. В. Богуш, В. Д. Бровко, В. П. Настрадін; під. ред. В. М. Богуша. — К.: Видавництво Ліра-К, 2020. — 554 с.
2. Даник Ю.Г. Основи кібербезпеки та кібероборони: підручник / Ю.Г. Даник, П.П. Воробієнко, В.М. Чернега. – [Видання друге, перероб. та доп.]. – Одеса.: ОНАЗ ім. О.С. Попова, 2019. − 320 с.
3. Про основні засади забезпечення кібербезпеки України: Закон України (зі змінами) від 05.10.2017 р. № 2163-VIII. Дата оновлення: 08.07.2018.
4. ДСТУ ISO/IEC 27001:2015. Інформаційні технології. Методи захисту системи управління інформаційною безпекою. (ISO/IEC 27001:2013; Cor 1:2014, IDT) [Чинний від 2017-01-01]. Вид. офіц. Київ: ДП “УкрНДНЦ”. 2016. 22 с.
5. ДСТУ ISO/IEC 27005:2015(ISO/IEC 27005:2011, IDT)Інформаційні технології. Методи захисту.Управління ризиками інформаційної безпеки,2017. 65 с.
6. Вдовенко С., Даник Ю., Фараон С. Дефініційні проблеми термінології у сфері кібербезпеки і кібероборони та шляхи їх вирішення. CS&CS, 2019. Issue 1(13). С.17-29.

Додаткова:

1. Остроухов В.В., Петрик В.М., Присяжнюк М.М. та ін. Інформаційна безпека: соціально-правові аспекти: підручник; за заг.ред. Скулиша Є.Д. 2010. 512 с.
2. Кузьменко Б.В., Заіка Ю.О. Кібертероризм: світові й українські реалії // Науковий вісник Академії внутрішніх справ. 2012. № 2(81). С. 92-98.

Web-ресурси:

1. Castro D. (2018). Boosting the Cyberworkforce. URL: http://www.govtech.com/data/Boosting-the-Cyberworkforce.html.

2. Warsaw Summit Communiqué. Issued by the Heads of State and Government participating in the meeting of the North Atlantic Council in Warsaw 8-9 July 2016 09 Jul. 2016 - Press Release (2016) 100 Issued on 09 Jul. 2016 Last updated: 29 Mar. 2017 10:55 URL: https://www.nato.int/cps/en/natohq/official_texts_133169.htm?selectedLocale=en

3. Про національну безпеку України: Закон України від 21.06.2018 р. № 2469-VIII. URL: https://zakon.rada.gov.ua/laws/show/2469-19/ed20180621#n24.

4. Про Стратегію кібербезпеки України: Указ Президента України від 15.03.2016 р. №96/2016. URL: https://zakon.rada.gov.ua/laws/show/96/2016.

5. Технологія VPN може загрожувати кібербезпеці. URL: https://detector.media/infospace/article/126505/2017-05-31-tekhnologiya-vpn-mozhe-zagrozhuvati-kiberbezpetsi-inau/.