ЧЕРКАСЬКИЙ ДЕРЖАВНИЙ ФАХОВИЙ БІЗНЕС-КОЛЕДЖ РІК ЗАСНУВАННЯ - 1966

Відділення бакалаврської підготовки

Кафедра фінансового моніторінгу та підприємництва

СИЛАБУС

Базова інформація про дисципліну	
Назва дисципліни	CE112 Вступ до Кібербезпеки / Introduction to Cybersecurity
Рівень вищої освіти	Перший (бакалаврський) рівень
Галузь знань	07 Управління та адміністрування
Спеціальність	071 «Облік і оподаткування»
Освітньо-професійна програма	Облік і аудит
Семестр	7
Курс	3 (зі скороченим терміном навчання на базі ОКР фаховий молодший бакалавр)
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=856
Мова викладання	українська
Лектор курсу	Викладач Бреус Р.В. канали комунікації: СДН «Moodle»: повідомлення в чаті E-mail: breus.roksolana@gmail.com
Місце дисципліни в освітній програмі	
Освітньо-професійна програма	Облік і аудит
Перелік загальних компетентностей (ЗК)	Здатність вчитися і оволодівати сучасними знаннями. Здатність працювати в команді. Здатність працювати автономно. Навички використання сучасних інформаційних систем і комунікаційних технологій.
Перелік спеціальних компетентностей (СК)	-

Базова інформація про дисципліну	
Назва дисципліни	CE112 Вступ до Кібербезпеки / Introduction to Cybersecurity
Рівень вищої освіти	Перший (бакалаврський) рівень
Галузь знань	07 Управління та адміністрування
Перелік програмних результатів навчання	Застосовувати спеціалізовані інформаційні системи і комп'ютерні технології для обліку, аналізу, контролю, аудиту та оподаткування. Вміти працювати як самостійно, так і в команді, проявляти лідерські якості та відповідальність у роботі, дотримуватися етичних принципів, поважати індивідуальне та культурне різноманіття.
Опис дисципліни	
Структура навантаження на студента	Загальна кількість годин – 90 Кількість кредитів – 3 Кількість лекційних годин – 22 Кількість практичних занять – 23 Кількість годин для самостійної роботи студентів – 45 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. Основні положення забезпечення кібербезпеки.	Сутність кібербезпеки інформаційного суспільства. Кібербезпека як складова міжнародної, регіональної та національної безпеки.
Тема 2. Сутність кібербезпеки інформаційного суспільства. Загрози у сфері кібербезпеки.	Кібербезпека як складова міжнародної, регіональної та національної безпеки. Кіберінциденти: передумови скоєння та наслідки. 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 3. Основи міжнародної співпраці з питань забезпечення кібербезпеки. Напрями забезпечення кібербезпеки України	Проблеми забезпечення кібербезпеки на міжнародному рівні. Діяльність Міжнародного союзу електрозв'язку щодо забезпечення кібербезпеки. Напрями міжнародного співробітництва з питань забезпечення кібербезпеки. 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 4. 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-

Базова інформація про дисципліну	
Назва дисципліни	CE112 Вступ до Кібербезпеки / Introduction to Cybersecurity
Рівень вищої освіти	Перший (бакалаврський) рівень
Галузь знань	07 Управління та адміністрування
	телекомунікаційні системи та інформаційні ресурси. Характеристика APT-кібератак як основної форми боротьби в кіберпросторі.
Тема 5. 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 6. 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 7. Практичні аспекти забезпечення кібербезпеки	Основи організації підготовки фахівців з кібербезпеки. Аналіз досвіду провідних країн світу з підготовки фахівців кібербезпеки.
Тема 8. 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 9. 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 10. Оцінки інформаційних ризиків та управління ними.	Способи оцінки інформаційних ризиків. Сучасні підходи до оцінки ризиків інформаційних технологій.
Тема 11. Кіберзброя.	Сутність та призначення кіберзброї. Класифікація кіберзброї. 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.
Використання ШІ	Використання ШІ під час виконання завдань регламентується Політикою «Використання ШІ в освітньому процесі ЧДБК» Завдання мають маркування регламенту використання ШІ.

Базова інформація про дисципліну	
Назва дисципліни	CE112 Вступ до Кібербезпеки / Introduction to Cybersecurity
Рівень вищої освіти	Перший (бакалаврський) рівень
Галузь знань	07 Управління та адміністрування
Підсумковий контроль	Залік у кінці семестру за результатами поточної успішності.

Система оцінювання

Система оцінювання підсумкової успішності студентів поділяється на **поточний контроль** та **семестровий контроль**.

Поточний контроль здійснюється протягом семестру і охоплює всі види аудиторної роботи (практичні заняття) та виконання індивідуальних завдань. Максимальна кількість балів, яку студент може набрати за цей вид контролю, становить 100.

Підсумковий контроль

Відбуватися у формі заліку.

Розрахунок підсумкової оцінки

Підсумкова оцінка базується виключно на балах, накопичених протягом семестру (S). Ваговий коефіцієнт у цьому випадку становить 1.

Формула: O=S×1

Накопичування балів з навчальної дисципліни: поточний контроль	
Види навчальної роботи	**Загальна кількість балів**
Практична робота за темами 1 по 8 балів	**40**

Модульні контрольні (2 к.р. по 15 балів)	**30**
Індивідуальна самостійна робота (проєкт)	**30**
Разом	**100**

Критерії оцінювання для кожного виду навчальної

Критерії практичних робіт

8 б. – Студент виконав всі завдання практичної роботи без помилок, а також правильно оформив звіт.
7-6 б. – Студент виконав всі завдання практичної роботи, але є неточності та допустився помилок в оформленні звіту.
5-3 б. – Студент виконав всі завдання практичної роботи, але допустився помилок в них та є недоліки в оформленні звіту.
2 б. – Студент виконав лише частину завдань практичної роботи, але має помилки при виконанні, а також є недоліки в оформленні звіту.
1 б. – Студент намагався виконати практичну роботу, але в завданнях є помилки та звіт оформлено невірно.
0 б. – студент не виконав практичної роботи та не здав звіт.

Критерії оцінювання модульних робіт

15 б. – виконано всі 5 завдань без помилок, відповіді повні й обгрунтовані.
14-13 б. – виконано майже всі завдання, допущено декілька незначних помилок.
12-10 б. – виконано більшу кількість завдань, але є окремі помилки та недоречності у відповідях.
9-8 б. – виконано три завдання, але з помітними помилками.
7 б. – виконано два завдяння повністю та половину третього, але частина з них має помилки.
6 б. – виконано два завдання, але продемонстровано розуміння основного матеріалу.
5-4 б. – виконано деякі завдання правильно, але більшість з помилками.
3 б. – робота має лише деякі правильні елементи у відповідях.
2 б. – виконано мінімальний обсяг завдань, знання без глибокого розуміння.
1 б. – студент намагався виконати завдання, але відповіді містять помилки й потребують корекції.
0 б. – студент не виконав модульної контрольної роботи.

Критерії оцінювання індивідуальних робіт (проєктів)

30-29б – завдання виконано повністю, без жодної помилки; звіт правильно й акуратно оформлений, відповіді повні, логічні та аргументовані, можливі несуттєві помилки, але одиничні.
25-28б. – завдання виконано повністю, з незначними помилками; звіт оформлений на достатньому рівні, але є недоречності в оформленні.
24-20 б. – усі завдання виконані, але є несуттєві неточності у відповідях чи оформленні.
19–15 б. – виконано більшість завдань правильно, звіт загалом оформлений належно; наявні окремі помилки у змісті або дрібні недоліки в структурі/оформленні.
14–13 б. – завдання виконані частково, відповіді містять суттєві неточності чи неповноту; у звіті є помилки в оформленні або бракує аргументації.
12–10 б. – виконано половину чи трохи більше завдань, відповіді часто неправильні або поверхові; звіт має помітні недоліки у змісті та структурі.
9–7 б. – зроблено спробу виконати більшість завдань, проте більшість відповідей неправильні або неповні; звіт оформлено формально, із значними помилками.
6–4 б. – завдання виконані частково, правильних відповідей небагато; звіт майже не відповідає вимогам оформлення.
3–1 б. – зроблено лише символічну спробу виконати завдання; відповіді в основному неправильні; звіт оформлено вкрай слабко.
0 б. – завдання не виконано, звіт відсутній.

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. 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.

Інтернет 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/.