ЧЕРКАСЬКИЙ ДЕРЖАВНИЙ ФАХОВИЙ БІЗНЕС-КОЛЕДЖ РІК ЗАСНУВАННЯ - 1966

Відділення бакалаврської підготовки

Кафедра інформаційних, мультимедійних технологій та дизайну

СИЛАБУС

Базова інформація про дисципліну	
Назва дисципліни	CE104 / Захист інформації в комп'ютерних системах та мережах / Protection of Information in Computer Systems and Networks
Рівень вищої освіти	Перший (бакалаврський) рівень
Галузь знань	F Інформаційні технології
Спеціальність	F7 Комп'ютерна інженерія
Освітньо-професійна програма	Комп'ютерна інженерія
Семестр	3
Курс	2 (зі скороченим терміном навчання на базі ОКР фаховий молодший бакалавр)
Анотація курсу	Навчальна дисципліна спрямована на формування уявлення про методи забезпечення надійності та захисту інформаційних ресурсів, комплекс вимог до системи забезпечення безпеки комп'ютерних систем, методи аналізу впливу загроз безпеки на комп'ютерні системи та мережі ефективний вибір та застосування засобів захисту, розробка стратегії та політик безпеки комп'ютерної системи.
Сторінка курсу в MOODLE	http://78.137.2.119:2929/course/view.php?id=672
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	
Освітньо-професійна програма	Комп'ютерна інженерія
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.

Базова інформація про дисципліну	
Назва дисципліни	СЕ104 / Захист інформації в комп'ютерних системах та мережах / Protection of Information in Computer Systems and Networks
Рівень вищої освіти	Перший (бакалаврський) рівень
Галузь знань	F Інформаційні технології
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 – 240 Кількість кредитів – 8 Кількість лекційних годин – 60 Кількість практичних занять – 60 Кількість годин для самостійної роботи студентів – 120 Форма підсумкового контролю – залік, екзамен
Методи навчання	Розповідь, Пояснення, Бесіда, Інструктаж, Дискусія, Практична робота, Пробні вправи, Творчі вправи, Усні вправи, Практичні вправи.
Зміст дисципліни	
Тема 1. Проблеми та напрямкизабезпечення захисту в комп'ютерних системах (КС).	Напрямки забезпечення захисту КС. Політика безпеки, види політик безпеки. Загрози безпеки інформації та канали проникнення в систему. Основні вразливі місця комп'ютерних систем.
Тема 2. Стратегії захисту інформації, характеристики стратегій	Оборонна, наступальна, випереджуюча стратегії захисту ресурсів КС. Побудова систем захисту КС відповідно стратегій захисту
Тема 3. Методи і засоби захисту інформаційних ресурсів комп'ютерних систем	Правові та організаційні методи захисту інформації комп'ютерних систем. Криптографічний захист даних. Програмні методи захисту інформації. Фізичні методи і захисту інформації комп'ютерних систем.
Тема 4. Суть та елементи теорії надійності	Загальні положення теорії надійності. Відмова і її види. Комплексні показники надійності. Показники довговічності та збережності. Визначення показників надійності – інтенсивності, частоту та ймовірність відмов.
Тема 5. Показники та фактори, що впливають на надійністьКС та комп'ютерних мереж	Фактори, що впливають на функціональну надійність. Об'єктивні та суб'єктивні фактори, що пливають на надійність обладнання систем.

Базова інформація про дисципліну	
Назва дисципліни	CE104 / Захист інформації в комп'ютерних системах та мережах / Protection of Information in Computer Systems and Networks
Рівень вищої освіти	Перший (бакалаврський) рівень
Галузь знань	F Інформаційні технології
Тема 6. Підвищення надійності та захищеності КС	Основні аспекти підвищення надійності, методи (структурне, функціональне, часове, інформаційне, навантажувальне резервування) та їх ознаки. Визначення функції та коефіцієнт готовності відновлюваної системи за умови, що на неї діють прості потоки відмов і відновлень. Підвищення надійності систем. Резервування
Тема 7. Захист програмного забезпечення комп‘ютерних систем	Категорії засобів захисту програмного забезпечення. Програмні засоби захисту комп‘ютерних систем. Основні показники надійності ПЗ. Моделі надійності ПЗ.
Тема 8. Принципи забезпечення безпеки комп’ютерних мереж	Надійність та відмова мережі. Методики визначення критеріїв надійності математичної моделі КМ.
Тема 9. Ідентифікація та аутентифікація користувачів	Поняття про ідентифікацію користувача та її особливості. Основні принципи та методи аутентифікації. Біометрична аутентифікація. Схеми аутентифікаціїї та перевірки істиності
Тема 10. Моделювання систем захисту інформаційних ресурсів	Предмет, об’єкт захисту. Класифікація порушників безпеки. Принципи моделювання систем захисту інформації.Модель системи безпеки з повним перекриттям. Модель багаторівневого захисту інформації та інші.
Тема 11. Криптологічний захист інформаційних ресурсів	Основні терміни та поняття. Криптографічні методи захисту інформації. Сучасні криптосистеми та їх особливості. Симетричні алгоритми шифрування інформації. Системи з відкритим ключем. Цифрові підписи. Адміністрування ключами.
Тема 12. Принципи побудови захищених систем. Стандарти із захисту інформації	Архітектура захищених операційних систем. Критерії безпеки комп'ютерних систем Методи і засоби захисту від атак через мережу Internet. Основні схеми мережного захисту на базі міжмережевих екранів Захист електронної пошти. Забезпечення безпеки електронних платежів. Світові стандарти із захисту даних в комп'ютерних системах. Державний стандарт України із захисту інформації.

Базова інформація про дисципліну	
Назва дисципліни	СЕ104 / Захист інформації в комп'ютерних системах та мережах / Protection of Information in Computer Systems and Networks
Рівень вищої освіти	Перший (бакалаврський) рівень
Галузь знань	F Інформаційні технології
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.
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 1-6 по 8 балів	**20**
Практична робота за темами 7-12 по 8 балів	**20**
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 б. – завдання виконано повністю, без жодної помилки; звіт правильно й акуратно оформлений, відповіді повні, логічні та аргументовані.

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.

Критерії оцінювання іспиту
Іспит складається з блоку тестів (25 питань) та двох задач. В тестах лише одна правильна відповідь, кожна з яких оцінюється в 2 бали.
Кожна задача оцінюється в 25 балів:
20-25 б. Студент правильно розв'язав практичне завдання (задачу), спроможний пояснити методику її розв'язання та зміст застосовуваного понятійного апарату та формул.
15-19 б. Студент правильно розв'язав практичне завдання (задачу), але не в повній мірі розкрита методика її розв'язання та зміст застосовуваного понятійного апарату та формул.
10-14 б. Студент правильно розв'язав практичне завдання (задачу), але має несуттєві помилки при рішенні, не в повній мірі розкрита методика її розв'язання.
5-9 б. Задача вирішена не вірно, але чітко простежується правильний хід, логіку та послідовність рішення.
0-4 б. Задача вирішена не вірно, але простежується правильний хід та послідовність рішення.
0 б. Невірно вирішена задача.

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. 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.
2. Інформаційна безпека держави: навчальний посібник/ В.І. Гур'єв, .Б. Мехед, Ю.М. Ткач, І.В. Фірсова. – Ніжин: ФОП Лук'яненко В.В. ТПК,«Орхідея», 2018. 166 с.
3. Cyber Security for Cyber Physical Systems / Saqib Ali, Taiseera Al Balushi, Zia Nadir,

Omar Khadeer Hussain. – Cham, Switzerland : Springer, 2018. 174 p.
4. Хорошко В. О. 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.
5. 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.
6. 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.
7. 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.
8. ДСТУ ISO/IEC 27005:2015(ISO/IEC 27005:2011, IDT) Інформаційні технології. Методи захисту.Управління ризиками інформаційної безпеки, 2017. 65 с.
9. Security and Privacy inInternet of Things (IoTs): Models, Algorithms, and mplementations / Edited by Fei Hu. – Taylor & Francis Group, 2016. 564 p.

1. Інтернет ресурси

1. 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.
2. Про Стратегію кібербезпеки України: Указ Президента України від 15.03.2016 р. №96/2016. URL: https://zakon.rada.gov.ua/laws/show/96/2016.