

СИЛАБУС

Базова інформація про дисципліну	
Назва дисципліни	СЕ029 / Цифрова безпека / Digital Security
Рівень фахової передвищої освіти	Фаховий молодший бакалавр
Галузь знань	05 «Соціальні та поведінкові науки»
Спеціальність	051 «Економіка»
Освітня програма	Економіка
Семестр	4 семестр (2 курс 9 кл.)
Курс	2 курс (на базі базової середньої освіти)
Анотація курсу	Навчальна дисципліна зосереджена на вивченні складових цифрової безпеки та захисту інформації, а також їх класифікації та характеристики. В процесі вивчення курсу студенти ознайомляться з сучасними програмно-технічними засобами забезпечення цифрової безпеки; навчатися виявляти основні загрози цифрової безпеки, аналізувати і використовувати типові криптографічні засоби та методи захисту інформації, у тому числі електронний цифровий підпис, антивірусний захист.
Сторінка курсу в MOODLE	http://78.137.2.119:2929/course/view.php?id=791
Мова викладання	українська
Лектор курсу	Бреус Р.В., викладач канали комунікації: СДН «Moodle»: повідомлення в чаті E-mail: breus.roksolana@gmail.com
Місце дисципліни в освітній програмі	
Освітньо-професійна програма	http://csbc.edu.ua/documents/otdel/moop124_e.pdf
Перелік загальних компетентностей (ЗК)	ЗК 5. Здатність до пошуку, оброблення та аналізу інформації з різних джерел. ЗК 6. Здатність застосовувати знання у практичних ситуаціях. ЗК 7. Здатність використовувати інформаційні та комунікаційні технології.
Перелік спеціальних компетентностей (СК)	-
Перелік програмних результатів навчання	РН 5. Використовувати сучасні інформаційні і комунікаційні технології для розв'язання професійних завдань. РН 16. Використовувати сучасні інформаційні та комунікаційні технології для проведення аналітичних досліджень, підготовки та представлення звітів.
Опис дисципліни	

Структура навантаження на студента	Загальна кількість годин – 90 Кількість кредитів – 3 Кількість лекційних годин – 14 Кількість практичних занять – 16 Кількість годин для самостійної роботи студентів – 60 Форма підсумкового контролю – диференційний залік
Методи навчання	Розповідь, Пояснення, Бесіда, Інструктаж, Дискусія, Практична робота, Пробні вправи, Творчі вправи, Усні вправи, Практичні вправи.
Зміст дисципліни	
Тема 1. Вступ до дисципліни цифрова безпека.	Вступ до цифрової безпеки. Основні загрози цифровій безпеці. Принципи безпеки в цифровому середовищі. Інструменти та методи захисту. Безпека в Інтернеті та соціальних мережах. Безпека мобільних пристроїв.
Тема 2. Основні загрози для безпеки інформації та способи їхнього подолання.	Основні поняття та визначення. Типи загроз безпеки інформації. Класифікація загроз за методами впливу. Шкідливі програми та їх види. Загрози через людський фактор. Загрози для конфіденційності, цілісності та доступності інформації. Захист від загроз безпеки інформації.
Тема 3. Методи аутентифікації та управління доступом до інформаційних систем.	Основні поняття та визначення. Основні методи аутентифікації. Типи управління доступом. Принципи мінімальних привілеїв та необхідного доступу. Технології аутентифікації та управління доступом.
Тема 4. Особливості безпечного зберігання даних.	Основні поняття та визначення. Методи зберігання даних. Шифрування даних як метод захисту. Контроль доступу до даних. Резервне копіювання даних. Захист даних від фізичних загроз. Використання технологій для захисту даних. Використання технологій для захисту даних.
Тема 5. Забезпечення безпеки в комп'ютерних мережах.	Основні поняття та визначення. Типи загроз в мережах. Механізми захисту мереж. Шифрування та захист передавання даних. Контроль доступу в мережах. Безпека в бездротових мережах.
Тема 6. Соціальна інженерія та правила безпечного використання соціальних мереж.	Основні поняття та визначення. Методи соціальної інженерії. Методи захисту від соціальної інженерії. Правила безпечного використання соціальних мереж. Основи безпеки при публікаціях у соціальних мережах. Ризики використання соціальних мереж для компаній та організацій. Інструменти та технології для захисту у соціальних мережах.
Тема 7. Безпека програмного забезпечення та резервне копіювання і відновлення даних.	Основні поняття та визначення. Основи безпеки програмного забезпечення. Резервне копіювання даних. Відновлення даних. Інтеграція безпеки програмного забезпечення та резервного копіювання. Управління ризиками та найкращі практики.
Тема 8. Нові напрямки в галузі цифрової безпеки.	Основні поняття та визначення. Інтеграція штучного інтелекту та машинного навчання. Захист даних у хмарних середовищах. Загроза кіберзлочинності та нові види атак. Біометрична аутентифікація та багатофакторна аутентифікація. Захист персональних даних та відповідність регламентам (GDPR, CCPA).

	Інтернет речей (IoT) та його безпека.
Політика дисципліни	
Політика відвідування	Регулярне відвідування всіх видів занять, своєчасність виконання самостійної роботи. За об'єктивних причин студент може отримати індивідуальний графік навчання за погодженням із керівником курсу, завідувачем ЦК та завідувачем відділення.
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	Диференційний залік у кінці семестру за результатами поточної успішності (у формі підсумкового модульного контролю).

Візуальні індикатори використання ШІ в освітньому процесі ЧДБК: 2025



- ШІ має бути використаний для створення результатів, і студент повинен повідомити, як саме його використав.
- Невикористання ШІ вплине на оцінювання



- Результат має бути створений без допомоги ШІ, студент має використовувати лише власні знання та навички.
- Використання ШІ буде розцінено як академічна недоброчесність.



- ШІ може бути використаний при створенні результатів, студент зобов'язаний повідомити про його використання.
- Нерозкриття використання ШІ розцінюється як шахрайство, а використання ШІ може вплинути на оцінювання



- ШІ може бути вільно використаний для створення результатів, без обов'язкового повідомлення
- Використання ШІ не впливає на оцінювання

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

Відбувається у формі диференційного заліку (у формі підсумкового модульного контролю)

Розрахунок підсумкової оцінки

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

Формула: $O=S \times 1$

Види навчальної роботи	Загальна кількість балів
Усні відповіді за темами 1 по 3 балів	24
Практична робота за темами 1 по 6 балів	24
Модульні контрольні роботи (2 к.р. по 10 балів)	20
Тестування (2 тестування по 6 балів)	12
Індивідуальна самостійна робота (проект)	20
Разом	100

Критерії оцінювання для кожного виду навчальної

Критерії оцінювання усних відповідей:

- 3 б. – Студент відповів на всі питання правильно
- 2 б. – Студент відповів лише на декілька відповідей правильно.
- 1 б. – Студент відповів правильно лише на одне запитання.
- 0 б. – Студент не зміг відповісти на жодне запитання.

Критерії практичних робіт

- 6 б. – Студент виконав всі завдання практичної роботи без помилок, а також правильно оформив звіт.
- 5 б. – Студент виконав всі завдання практичної роботи, але допустився помилок в оформленні звіту.
- 4 б. – Студент виконав всі завдання практичної роботи, але допустився помилки в одному з них.
- 3 б. – Студент виконав всі завдання практичної роботи, але допустився помилки в двох з 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

- 10 б. – виконано всі 5 завдань без помилок, відповіді повні й обґрунтовані.
- 9 б. – виконано майже всі завдання, допущено декілька незначних помилок.
- 8 б. – виконано більшу кількість завдань, але є окремі помилки та недоречності у відповідях.
- 7 б. – виконано три завдання, але з помітними помилками.
- 6 б. – виконано два завдання повністю та половину третього, але частина з них має помилки.
- 5 б. – виконано два завдання, але продемонстровано розуміння основного матеріалу.
- 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.

Критерії оцінювання індивідуальних робіт (проектів)

20 б. – завдання виконано повністю, без жодної помилки; звіт правильно й акуратно оформлений, відповіді повні, логічні та аргументовані.

19 б. – усі завдання виконані, але є 1–2 несуттєві неточності у відповідях чи оформленні.

18–15 б. – виконано більшість завдань правильно, звіт загалом оформлений належно; наявні окремі помилки у змісті або дрібні недоліки в структурі/оформленні.

4–13 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 слабо.

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. Пошук і обробка інформації професійного спрямування: навч. посіб. / Н. М. Титова, Н. М. Рідей, В. П. Настрadin, М. М. Присяжнюк ; за заг. ред. Н. М. Титової. Київ : Ліра-К, 2024. – 136 с.
2. Титова Н. М. Інформаційна безпека та кібербезпека держави : навч. посіб. / Н. М. Титова, Н. М. Рідей, В. П. Настрadin, М. М. Присяжнюк, С. М. Мамченко, С. В. Артюх, Р. О. Яворська. Київ : Ліра-К, 2024. 224 с.
3. Полторак В. П., Савчук О. В. Інформаційна безпека та захист даних в комп'ютерних технологіях і мережах. Вибрані розділи: навч. посіб. Київ: КПІ ім. Ігоря Сікорського, 2021. 384 с. URL: <https://ela.kpi.ua/handle/123456789/47380>
4. Титова Н. М., Рідей Н. М., Настрadin В. П., Присяжнюк М. М., Мамченко С. М., Артюх С. В., Яворська Р. О. Інформаційна безпека та кібербезпека держави: навч. посіб. – Київ: Ліра-К, 2024. 224 с.
5. Соловйов В. М., Кузнецов С. Д. Кібербезпека: основи захисту інформації в інформаційно-комунікаційних системах: навч. посіб. – Київ: Національний авіаційний університет, 2020. 256 с.
6. Гнатюк С. М., Коваленко А. О. Основи кібербезпеки: навч. посіб. – Київ: Вид-во

НТУУ «КПІ ім. Ігоря Сікорського», 2019. 312 с.

7. Петренко О. В., Іванов І. І. Захист інформації в комп'ютерних системах: підручник. Харків: ХНУРЕ, 2021. 348 с.
8. Сидоренко В. В., Мельник М. М. Кібербезпека та захист інформації: навч. посіб. – Львів: Львівська політехніка, 2022. 290 с.
9. Кравченко П. П., Литвиненко О. О. Інформаційна безпека: сучасні аспекти та технології: монографія. Одеса: ОНПУ, 2020. 275 с.
10. Дерев'янка Б. – В., Шевченко О. В. Кіберзахист критичної інфраструктури: метод. рекомендації. Київ: Держспецзв'язку, 2021. 88 с.
11. Морозов А. В., Кузьменко О. С. Технології забезпечення інформаційної безпеки: навч. посіб. – Дніпро: ДНУ ім. Олеса Гончара, 2019. 234 с.
12. Федоренко В. Г., Соколовський С. В. Кібербезпека: теорія та практика: підручник. Київ: КНЕУ, 2023. 320 с.
13. Литвиненко В. В., Гончарук С. М. Основи інформаційної безпеки: навч. посіб. Харків: ХНУ ім. В. Н. Каразіна, 2021. 298 с.
14. Бондаренко С. В., Ковальчук О. П. Кібербезпека в державному управлінні: монографія. Київ: НАДУ, 2022. 310 с.

Інтернет ресурси

1. Головка Д. Ю. Безпека в цифровому просторі : електронний навчальний курс / Д. Ю. Головка. – Біла Церква : БІНПО ДЗВО «УМО» НАПН України, 2024. – 54 с. URL: <https://lib.iitta.gov.ua/id/eprint/739432/1/%D0%95%D0%9D%D0%9A%20%D0%91%D0%B5%D0%B7%D0%BF%D0%B5%D0%BA%D0%B0%20%D0%B2%20%D0%A6%D0%9F.pdf>
2. Державна служба спеціального зв'язку та захисту інформації України. Методичні рекомендації щодо підвищення рівня кіберзахисту систем електронного документообігу. 2023. URL: <https://cybersec.net.ua/normativni-dokumenty/591-metodychni-rekomendatsii-shchodo-pidvyshchennia-rivnia-kiberzakhystu-system-elektronnoho-dokumentobihu-vid-derzhspetsviazku.html>
3. Адміністрація Держспецзв'язку. Методичні рекомендації щодо підвищення рівня кіберзахисту систем електронного документообігу: наказ від 30.08.2023 № 773. URL: <https://zakon.rada.gov.ua/go/v0773519-23>
4. Почапська О. І. (Не)безпека в цифровому світі: навчальний посібник / О. І. Почапська. Київ : Академія української преси, Центр вільної преси, 2024. 59 с.
5. Тарнавський Ю. А. Безпека інформаційних систем: підручник для студ. спеціальності 122 «Комп'ютерні науки», освітня програма «Цифрові технології в енергетиці». Київ: КПІ ім. Ігоря Сікорського, 2023. 163 с. URL: <https://ela.kpi.ua/handle/123456789/62709>.