



СИЛАБУС НАВЧАЛЬНОЇ ДИСЦИПЛІНИ

ОСНОВИ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ ТА ЗАХИСТУ ІНФОРМАЦІЇ

ID 6197

Шифр, назва спеціальності та освітній рівень	071 Облік і оподаткування (бакалавр)	Назва освітньої програми	Діджитал-облік та консалтинг (2024)
Тип програми	Освітньо-професійна	Мова викладання	Українська
Факультет	Факультет комп'ютерно-інформаційних систем і програмної інженерії (ФІС)	Кафедра	Каф. кібербезпеки (КБ)

Викладач/викладачі

Деркач Марина Володимирівна, канд. техн. наук, доцент, доцент, [профіль на порталі "Науковці ТНТУ"](#)

Загальна інформація про дисципліну

Мета курсу	<p>Мета вивчення навчальної дисципліни: набуття теоретичних та практичних знань для планувати безпечної роботи на персональному комп'ютері, визначення вразливих місць персонального комп'ютера в умовах функціонування глобальної мережі, уміння роботи з програмним забезпеченням для захисту, відновлення та знищення даних на електронних носіях.</p> <p>Завдання навчальної дисципліни: оволодіння знаннями з основ інформаційної безпеки комп'ютерних систем, проблемами захисту інформації та підходами до їх розв'язання.</p>
Формат курсу	<p>Дисципліна передбачає проведення лекційних, практичних занять та консультацій. Для кращого розуміння та засвоєння викладеного матеріалу дисципліна має супровід у вигляді електронного курсу Тернопільський національний технічний університет ім. І. Пулюя (https://dl.tntu.edu.ua). Електронні навчальні курси мають лекційний матеріал, практичні роботи та систему тестування.</p>
Компетентності ОП	<p>Загальні:</p> <p>ЗК01. Здатність вчитися і оволодівати сучасними знаннями.</p> <p>ЗК07. Здатність бути критичним та самокритичним.</p> <p>ЗК11. Навички використання сучасних інформаційних систем і комунікаційних технологій.</p> <p>ЗК12. Здатність діяти соціально відповідально та свідомо.</p> <p>Спеціальні (фахові):</p> <p>СК08. Ідентифікувати та оцінювати ризики недосягнення управлінських цілей суб'єкта господарювання, недотримання ним законодавства та регулювання діяльності, недостовірності звітності, збереження й використання його ресурсів.</p> <p>СК10. Здатність застосовувати етичні принципи під час виконання професійних обов'язків.</p>
Програмні результати навчання з ОП	<p>ПР12. Застосовувати спеціалізовані інформаційні системи і комп'ютерні технології для обліку, аналізу, контролю, аудиту та оподаткування.</p> <p>ПР20. Виконувати професійні функції з урахуванням вимог соціальної відповідальності, трудової дисципліни, вміння планувати та управляти часом.</p>
Обсяг курсу	<p>Очна (денна) форма здобуття освіти:</p> <p>Кількість кредитів ECTS — 5; лекції — 32 год.; практичні заняття — 32 год.; самостійна робота — 86 год.;</p> <p>Заочна форма здобуття освіти:</p> <p>Кількість кредитів ECTS — 5; лекції — 6 год.; практичні заняття — 6 год.; самостійна робота — 138 год.;</p>
Ознаки курсу	<p>Рік навчання — 2; семестр — 3; Вибіркова дисципліна; кількість модулів — 2;</p>
Форма контролю	<p>Поточний контроль: модульний контроль рівня засвоєння теоретичних знань та виконання лабораторних робіт</p> <p>Підсумковий контроль: залік</p>
Компетентності та дисципліни, що є передумовою для вивчення	<p>Студенти повинні володіти базовими знаннями комп'ютерних та інтернет технологій.</p>

СТРУКТУРА КУРСУ

Лекційний курс	Годин		
	ОФЗО	ЗФЗО	
Основні поняття інформаційної безпеки	4	2	
Основні загрози безпеки	4	2	
Механізми реалізації безпеки.	4	0	
Характеристика стандартів із забезпечення Інформаційної безпеки	4	0	
Ризик роботи на персональному комп'ютері	4	0	
Засоби захисту інформації	4	2	
Загальна характеристика комплексного захисту інформації	4	0	
Міжнародний стандарт безпеки ISO/IEC 17799	4	0	
	РАЗОМ:	32	6

Практичні заняття (теми)	Годин		
	ОФЗО	ЗФЗО	
Ізольований запуск програм у Windows. Пісочниця Windows	6	4	
Відновлення та знищення даних на електронних носіях	6	2	
Захист інформації в архівах	4	0	
Захист інформації на електронних носіях	8	0	
Робота з електронними цифровими підписами	8	0	
	РАЗОМ:	32	6

ІНШІ ВИДИ РОБІТ

Теми, короткий зміст

Самостійно опрацювати теми: основні нормативно-правові документи України у сфері ІБ, забезпечення безпеки об'єктів інформаційної сфери держави, засоби забезпечення ІБ в комп'ютерних системах. Виконати роботу по створенню та захисту даних в середовищі MS Excel.

Базова

1. Бурячок В.Л. Інформаційна та кібербезпека / В.Л. Бурячок, В.В. Толубко, В.О. Хорошко, С.В. Толюпа. – К.: ДУТ, 2015. – 288 с.
2. Нашинець-Наумова А.Ю. Інформаційна безпека: питання правового регулювання. – К.: ВД “Гельветика”, 2017. – 168 с
3. Основи інформаційних технологій і систем : підручник / В. А. Павлиш, Л. К. Гліненко, Н. Б. Шаховська. – Львів : Львівська політехніка, 2018. – 620 с.
4. Закон України «Про інформацію» від 02.10.1992 № 2657-ХІІ.
5. Закон України «Про захист інформації в інформаційно-телекомунікаційних системах» № 1089-ІХ від 16.12.2020.
6. Закон України «Про державну таємницю» від 21.01.1994 № 3855-ХІІ.
7. Закон України «Про захист персональних даних» від 01.06.2010 № 2297-ВІ.
8. ДСТУ ISO/IEC 27002:2023 Інформаційна безпека, кібербезпека та захист конфіденційності. Засоби контролювання інформаційної безпеки (ISO/IEC 27002:2022, IDT).
9. ДСТУ ISO/IEC 29146:2023 (ISO/IEC 29146:2016)/Зміна № 1:2023 (ISO/IEC 29146:2016/Amd 1:2022, IDT) Інформаційні технології. Методи безпеки. Структура керування доступом.

Допоміжна

1. Деркач М.В. Використання алгоритму шифрування AES-256-CBC для зберігання даних автентифікації автономного помічника / М.В. Деркач, О.Є. Мишко // Наукові вісті Далівського університету. Електронне видання. - №24. – 2023.
2. Деркач М.В. Розробка мобільного додатку для визначення автентичності медіа файлу / М.В. Деркач, В.Ю. Остопець, В.С. Дерев'янченко // Вісник Східноукраїнського національного університету імені Володимира Даля. – Київ: СНУ ім.В.Даля, 2023. – № 3(279). – С.5-10.
3. Деркач М.В. Тестування безпеки вебресурсу на базі інструментів для сканування та виявлення вразливостей / М.В. Деркач, В.Г. Хомишин, В.О. Гудзенко // Наукові вісті Далівського університету. Електронне видання. - №25. - 2023.
4. Mishko O., Matiuk D., Derkach M. (2024) Security of remote iot system management by integrating firewall configuration into tunneled traffic. Scientific Journal of TNTU (Tern.), vol 115, no 3, pp. 122–129.

ІНФОРМАЦІЙНІ РЕСУРСИ

1. ЕНК Основи інформаційної безпеки та захисту інформації ID: 6197 <https://dl.tntu.edu.ua/login.php?course=6197>
2. Міністерство освіти і науки України. URL: <http://mon.gov.ua/>
3. Національна наукова бібліотека ім. Вернадського. URL: <http://www.nbuv.gov.ua/>
4. Освіта.ua. URL: <http://osvita.ua/>
5. Форум інформатиків України. URL: <http://informatic.org.ua/>

Основні сайти з інформацією по дисципліні «Основи інформаційної безпеки та захисту інформації»

1. <https://www.coursera.org/learn/security-concepts-and-practices> - навчальний курс
2. <https://www.coursera.org/learn/data-privacy-and-protection-standards> - навчальний курс
3. <https://www.coursera.org/learn/introduction-to-cybersecurity-fundamentals> - навчальний курс
4. <https://www.coursera.org/learn/introduction-to-computer-security> - навчальний курс
5. <https://www.coursera.org/learn/codio-security-infrastructure-management> - навчальний курс

Політики курсу

індивідуальні консультації; екзамен. Можливий ректорський контроль.

Політика щодо
консультавання

Консультації при вивченні дисципліни проводяться згідно затвердженого на кафедрі . Консультавання передбачено як очно ,так і з використанням ресурсів електронного навчального курсу у середовищі електронного навчання університету.

Політика щодо
перескладання

Студент має право на повторне складання модульного контролю з метою підвищення рейтингу протягом тижня після складання модульного контролю за графіком. Перескладання екзамену відбувається в терміни, визначені графіком освітнього процесу. Здобувач ВО має право на зарахування результатів навчання здобутих у неформальній чи інформальній освіті.

Політика щодо академічної
добросовісності

При складанні усіх видів контролю у середовищі електронного навчання завжди активується система розпізнавання особи, що складає контроль. Усі практичні роботи у ЕНК перевіряються вбудованою системою Антиплагіат. При складанні усіх форм контролю забороняється списування, у тому числі з використанням сучасних інформаційних технологій.

Політика щодо відвідування

Відвідування занять є обов'язковим компонентом освітнього процесу. За наявності поважних причин (наприклад, хвороба, особливі потреби, відрядження, сімейні обставини, участь у програмах академічної мобільності тощо) навчання може здійснюватися за індивідуальним графіком, погодженим з деканом факультету.

СИСТЕМА ОЦІНЮВАННЯ

Розподіл балів, які отримують студенти за курс

Модуль 1			Модуль 2			Підсумковий контроль	Разом з дисципліни
Аудиторна та самостійна робота			Аудиторна та самостійна робота			Одна третя від суми балів, набраних здобувачем впродовж семестру	100
Теоретичний курс (тестування)	Практична робота		Теоретичний курс (тестування)	Практична робота			
20	21		20	14		25	
№ лекції	Види робіт	К-ть балів	№ лекції	Види робіт	К-ть балів		
Тема 1	Практичне заняття №1	7	Тема 5	Практичне заняття №4	7		
Тема 2	Практичне заняття №2	7	Тема 6	Практичне заняття №5	7		
Тема 3	Практичне заняття №3	7	Тема 7				
Тема 4			Тема 8				

Розподіл оцінок

Сума балів за навчальну діяльність

Шкала ECTS

Оцінка за національною шкалою

90-100

A

Відмінно

82-89

B

Добре

75-81

C

Добре

67-74

D

Задовільно

60-66

E

Задовільно

35-59

FX

Незадовільно з можливістю повторного складання

1-34

F

Незадовільно з обов'язковим повторним вивченням дисципліни

Затверджено рішенням кафедри КБ, протокол №1 від «29» серпня 2024 року.

ПОГОДЖЕНО

Гарант освітньої програми канд. екон. наук, доцент кафедри ОА

Тетяна КОРОЛЮК