СИЛАБУС НАВЧАЛЬНОЇ ДИСЦИПЛІНИ «ТЕХНОЛОГІЇ ЗАХИСТУ ДАНИХ В КОМП'ЮТЕРНИХ СИСТЕМАХ»

<table>
<tr><td colspan="3">Лектор курсу</td><td colspan="2">Коротков Сергій Станіславович,
доктор філософії, доцент</td><td colspan="2">Контактна інформація лектора (e-mail), сторінка курсу в Google</td><td colspan="2">e-mail: s.korotkov@duikt.edu.ua
сторінка курсу в Google Classroom –
https://classroom.google.com/c/ODM2NzU0MDgzNzA2?cjc=jg6tm37z</td></tr>
<tr><td colspan="3">Галузь знань</td><td colspan="2"></td><td colspan="2">Рівень вищої освіти</td><td colspan="2">магістр</td></tr>
<tr><td colspan="3">Спеціальність</td><td colspan="2"></td><td colspan="2">Семестр</td><td colspan="2"></td></tr>
<tr><td colspan="3">Освітня програма</td><td colspan="2"></td><td colspan="2">Тип дисципліни</td><td colspan="2">Цикл вибіркових компонент</td></tr>
<tr><td rowspan="2">Обсяг:</td><td>Кредитів ECTS</td><td>Годин</td><td colspan="6">За видами занять:</td></tr>
<tr><td>5</td><td>150</td><td>Лекцій
18</td><td>Семінарських занять
-</td><td>Практичних занять
36</td><td>Лабораторних занять
-</td><td colspan="2">Самостійна підготовка
96</td></tr>
<tr><td colspan="9">АНОТАЦІЯ КУРСУ</td></tr>
<tr><td colspan="9">Взаємозв’язок у структурно-логічній схемі</td></tr>
<tr><td colspan="3">Освітні компоненти, які передують вивченню</td><td colspan="6"></td></tr>
<tr><td colspan="3">Освітні компоненти для яких є базовою</td><td colspan="6"></td></tr>
<tr><td>Мета курсу:</td><td colspan="8">Формування у студентів теоретичних знань та практичних навичок у сфері захисту інформації, вивчення сучасних методів криптографії, стеганографії, а також засобів забезпечення конфіденційності, цілісності та доступності даних у комп'ютерних системах.</td></tr>
<tr><td colspan="9">Компетентності відповідно до освітньої програми</td></tr>
<tr><td colspan="4">Загальні компетентності</td><td colspan="5">Спеціальні (фахові) компетентності</td></tr>
<tr><td colspan="4">Здатність приймати обґрунтовані рішення.</td><td colspan="5">Здатність до визначення технічних характеристик, конструктивних особливостей, застосування і експлуатації програмних, програмно-технічних засобів, комп’ютерних систем та мереж різного призначення.
Здатність розробляти алгоритмічне та програмне забезпечення, компоненти комп’ютерних систем та мереж, Інтернет додатків, кіберфізичних систем з використанням сучасних методів і мов програмування, а також засобів і систем автоматизації проектування.
Здатність забезпечувати якість продуктів і сервісів інформаційних технологій на протязі їх життєвого циклу.
Здатність ідентифікувати, класифікувати та описувати роботу програмно-технічних засобів, комп’ютерних систем, мереж та їхніх компонентів.</td></tr>
<tr><td colspan="9">Програмні результати навчання</td></tr>
<tr><td colspan="9">Застосовувати спеціалізовані концептуальні знання, що включають сучасні наукові здобутки у сфері комп’ютерної інженерії, необхідні для професійної діяльності, оригінального мислення та проведення досліджень, критичного осмислення проблем інформаційних технологій та на межі галузей знань.
Аналізувати проблематику, ідентифікувати та формулювати конкретні проблеми, що потребують вирішення, обирати ефективні методи їх вирішення.
Застосовувати знання технічних характеристик, конструктивних особливостей, призначення і правил експлуатації програмно-технічних засобів комп’ютерних систем та мереж для вирішення складних задач комп’ютерної інженерії та дотичних проблем.
Розробляти програмне забезпечення для вбудованих і розподілених застосувань, мобільних і гібридних систем.
Приймати ефективні рішення з питань розроблення, впровадження та експлуатації комп’ютерних систем і мереж, аналізувати альтернативи, оцінювати ризики та імовірні наслідки рішень.</td></tr>
</table>

ОРГАНІЗАЦІЯ НАВЧАННЯ			
Тема, опис теми	**Вид заняття**	**Оцінювання за тему**	**Форми і методи навчання/питання до самостійної роботи**
Змістовний модуль 1. Криптографічні методи захисту інформації			
Тема 1. ***Вступ до захисту даних та інформаційної безпеки.*** ***Знати***: основні поняття ризиків та загроз, законодавчу базу. ***Вміти***: проводити аналіз ризиків. ***Рекомендовані джерела:*** 1-8			
Заняття 1.1 Вступ до захисту даних та інформаційної безпеки.	Лекція 1 2 год		Пояснювально-ілюстративний, лекція-бесіда, бліц-опитування
Заняття 1.2 Аналіз ризиків та розробка політики безпеки.	Практичне заняття 1 4 год	4 бали	Кейс-метод, робота в групах, дискусія
Тема 2. ***Симетрична криптографія.*** ***Знати***: алгоритми блокового та потокового шифрування. ***Вміти***: реалізовувати шифрування файлів програмно. ***Рекомендовані джерела:*** 1-8			
Заняття 2.1 Симетрична криптографія.	Лекція 2 2 год		Пояснювально-ілюстративний, лекція-візуалізація, бліц опитування
Заняття 2.2. Шифрування файлів.	Практичне заняття 2 4 год	4 бали	Колаборативне навчання, демонстрування, робота над помилками
Тема 3. ***Асиметрична криптографія*** ***Знати***: принципи роботи RSA, ECC. ***Вміти***: генерувати ключі та накладати ЕЦП. ***Рекомендовані джерела:*** 1-8			
Заняття 3.1 Асиметрична криптографія.	Лекція 3 2 год		Метод виокремлення основного, міні-лекція, бліц опитування
Заняття 3.2. Генерація Ключів та Цифрові Підписи.	Практичне заняття 3 4 год	4 бали	Колаборативне навчання, кейс-метод, мозгова атака, усне опитування
	Самостійна робота		
Тема 1. ***Вступ до захисту даних та інформаційної безпеки.***	12 год	4 бали	1. Технологія Blockchain та криптовалюти. Дослідження алгоритмів консенсусу та безпеки смарт-контрактів.
Тема 2. ***Симетрична криптографія.***	12 год	4 бали	2. Постквантова криптографія. Огляд алгоритмів, стійких до атак квантових комп'ютерів.
Тема 3. ***Асиметрична криптографія.***	12 год	4 бали	3. Стеганографічні методи. Програмна реалізація методу LSB для приховання тексту в зображенні

Тема 4. ***Криптографічні хеш-функції та цифрові сертифікати.*** ***Знати***: алгоритми хешування, структуру X.509, роботу PKI. ***Вміти***: створювати та перевіряти цифрові сертифікати. ***Рекомендовані джерела:*** 1 - 8			
Заняття 4.1 Криптографічні хеш-функції та цифрові сертифікати.	Лекція 4 2 год		Пояснювально-ілюстративний, лекція-бесіда, бліц опитування
Заняття 4.2 Робота з цифровими сертифікатами.	Практичне заняття 4 4 год	4 бали	Колаборативне навчання, кейс-метод
Змістовний модуль 2. Мережева безпека та захист інфраструктури			
Тема 5. ***Безпечні мережеві протоколи.*** ***Знати***: принципи роботи SSL/TLS, SSH, IPSec, VPN. ***Вміти***: аналізувати захищений трафік, налаштовувати тунелювання. ***Рекомендовані джерела:*** 1-8			
Заняття 5.1. Безпечні мережеві протоколи.	Лекція 5 2 год		Пояснювально-ілюстративний, лекція-бесіда, бліц опитування
Заняття 5.2. Захист мережевого трафіку.	Практичне заняття 5 4 год	4 бали	Дослідницький метод, аналіз кейсів
Тема 6. ***Ідентифікація, автентифікація та контроль доступу.*** ***Знати***: методи багатофакторної автентифікації, біометрію, Kerberos. ***Вміти*** налаштовувати системи автентифікації та права доступу. ***Рекомендовані джерела:*** 1-8			
Заняття 6.1 Ідентифікація, автентифікація та контроль доступу.	Лекція 6 2 год		Лекція-бесіда
Заняття 6.2. Налаштування систем автентифікації.	Практичне заняття 6 4 год	4 бали	Лабораторний практикум
Тема 7. ***Безпека веб-застосунків.*** ***Знати***: класифікацію вразливостей OWASP Top 10 (SQLi, XSS). ***Вміти***: проводити аудит веб-додатків та усувати вразливості. ***Рекомендовані джерела:*** 1-8			
Заняття 7.1 Безпека веб-застосунків.	Лекція 7 2 год		Пояснювально-ілюстративний, лекція-бесіда, бліц опитування
Заняття 7.2. Пошук та усунення вразливостей у веб-додатках.	Практичне заняття 7 4 год	4 бали	Колаборативне навчання, демонстрування, мозгова атака, робота над помилками

	Самостійна робота		
Тема 4. ***Криптографічні хеш-функції та цифрові сертифікати.***	12 год	2 бали	1. Міжнародні стандарти ІБ. Детальний аналіз сімейства стандартів ISO/IEC 27000. Розробка фрагменту політики безпеки згідно ISO 27001.
Тема 5. ***Безпечні мережеві протоколи.***	12 год	2 бали	2. Безпека хмарних обчислень. Модель спільної відповідальності в AWS/Azure.
Тема 6. ***Ідентифікація, автентифікація та контроль доступу.***	12 год	2 бали	3. Безпека Інтернету речей. Аналіз вразливостей протоколів MQTT та CoAP. Захист розумних пристроїв.
Тема 7. ***Безпека веб-застосунків.***	12 год	2 бали	4. Основи комп'ютерної криміналістики. Методи зняття образів дисків та аналізу оперативної пам'яті.
Змістовний модуль 3. Динамічні структури даних			
Тема 8. ***Системи виявлення вторгнень.*** ***Знати***: методи сигнатурного та евристичного аналізу, роботу Firewalls. ***Вміти***: розгортати IDS, аналізувати логи безпеки. ***Рекомендовані джерела:*** 1-8			
Заняття 8.1 Системи виявлення вторгнень (IDS/IPS).	Лекція 8 2 год		Пояснювально-ілюстративний, лекція-бесіда, бліц опитування
Заняття 8.2 Алгоритми обробки динамічних масивів даних.	Практичне заняття 8 4 год	4 бали	Колаборативне навчання, демонстрування, мозгова атака, робота над помилками
Тема 9. ***Стеганографія та приховання даних.*** ***Знати***: методи приховання інформації в медіаконтейнерах. ***Вміти***: використовувати стеганографічні утиліти, виявляти приховані дані. ***Рекомендовані джерела:*** 1-8			
Заняття 9.1 Стеганографія та приховання даних.	Лекція 9 2 год		Пояснювально-ілюстративний, лекція-бесіда, бліц опитування
Заняття 9.2 Стеганографічний захист інформації.	Практичне заняття 9 4 год	4 бали	Колаборативне навчання, демонстрування, мозгова атака, робота над помилками
	Самостійна робота		
Тема 8. ***Системи виявлення вторгнень.***	6 год	2 бали	1. Концепція Zero Trust. Принципи побудови архітектури "нульової довіри". Мікросегментація мережі.
Тема 9. ***Стеганографія та приховання даних.***	6 год	2 бали	2. Мікросегментація мережі..
МАТЕРІАЛЬНО-ТЕХНІЧНЕ ЗАБЕЗПЕЧЕННЯ ДИСЦИПЛІНИ			
• Мультимедійний проектор, інтерактивна дошка та/або віртуальна дошка. • Комп’ютерний клас для проведення практичних та лабораторних занять із встановленим програмним забезпеченням Visual Studio C++, Visual Studio C++.Net, Python, PyCharm, а також спеціалізованим ПЗ для захисту даних (OpenSSL, Wireshark, Snort). • Доступ до мережі Internet по роботі з онлайн-сервісами Lucidchart, Draw.io, OnlineGDB, Google Colaboratory.			

ІНФОРМАЦІЙНЕ ЗАБЕЗПЕЧЕННЯ ДИСЦИПЛІНИ

1. Євсеєв С. П., Шматко О. В., Ахієзер О. Б., Горбач Т. В. Основи кібербезпеки : навч.-практ. посібник. – Харків – Львів : "Новий Світ-2000", 2025. – 95 с. https://repository.kpi.kharkov.ua/handle/KhPI-Press/93101
2. Остапов С. Е., Євсеєв С. П., Король О. Г. Технології захисту інформації : навчальний посібник. – 2-ге вид., стер. – Львів : «Новий Світ-2000», 2020. – 678 с. https://ns2000.com.ua/tekhnolohii-zakhystu-informatsii-navchalnyy-posibnyk/
3. Інформаційна безпека та кібербезпека держави : навчальний посібник. – Київ : Ліра-К, 2024. – 224 с. https://lira-k.com.ua/products/informatsijna-bezpeka-ta-kiberbezpeka-derzhavy
4. Вишня В. Б., Гавриш О. С. Основи інформаційної безпеки : навчальний посібник. – Дніпро : Дніпроп. держ. ун-т внутріш. справ, 2020. – 128 с. https://er.dduvs.edu.ua/handle/123456789/4206
5. Горбенко І. Д., Горбенко Ю. І. Прикладна криптологія. Теорія. Практика. Застосування : підручник. – Харків : Форт, 2013. – 878 с.
6. Басюк Т. М., Думанський Н. О., Пасічник О. В. Основи інформаційних технологій : навчальний посібник. – Львів : «Новий Світ-2000», 2025. – 390 с. https://ns2000.com.ua/osnovy-informatsiynykh-tekhnolohiy-navchal-nyy-posibnyk/
7. Лаптєв О. А., Кривулькін І. М., Козленко В. В. Криптографія та криптоаналіз : підручник. – Київ : ВІТІ, 2019. – 320 с.
8. Методичні рекомендації до організації роботи, виконання, оформлення та захисту кваліфікаційної роботи магістра за спеціальністю 125 «Кібербезпека» / Уклад.: В. Л. Бурячок, В. Б. Толубко. – Київ : ДУІКТ, 2023. – 64 с. https://duikt.edu.ua/ua/lib/1/category/2185/view/548

ПОЛІТИКА КУРСУ («ПРАВИЛА ГРИ»)

- Курс передбачає роботу в колективі.
- Середовище в аудиторії є дружнім, творчим, відкритим до конструктивної критики.
- Освоєння дисципліни передбачає обов’язкове відвідування лекцій і практичних занять, а також самостійну роботу.
- Самостійна робота включає в себе теоретичне вивчення питань, що стосуються тем лекційних занять, які не ввійшли в теоретичний курс, або ж були розглянуті коротко, їх поглиблена проробка за рекомендованою літературою.
- Усі завдання, передбачені програмою, мають бути виконані у встановлений термін.
- Якщо студент відсутній з поважної причини, він презентує виконані завдання під час самостійної підготовки та консультації викладача.
- Під час роботи над завданнями не допустимо порушення академічної доброчесності: при використанні Інтернет ресурсів та інших джерел інформації студент повинен вказати джерело, використане в ході виконання завдання. Виявлення ознак академічної не доброчесності в практичній (письмовій) роботі студента є підставою для її не зарахування викладачем.
- Студент, який спізнився має право бути присутнім на занятті. Студенти мають інформувати старосту про неможливість відвідати заняття.
- Користування мобільним телефоном, планшетом чи іншими мобільними пристроями під час заняття в цілях не пов’язаних з навчанням є підставою для не зарахування викладачем роботи студента.

КРИТЕРІЇ ТА МЕТОДИ ОЦІНЮВАННЯ

Умовою допуску до підсумкового контролю є виконання всіх практичних робіт і виконання самостійних завдань, які передбачені структурою освітньої компоненти Технології захисту даних в комп'ютерних системах.

Якщо студента не допущено до складання заліку, як такого, що не виконав індивідуальний план, йому надається час до перескладання для виконання всіх вимог допуску. Студент має право на два перескладання. При повторному перескладанні екзамену у студента може приймати комісія, яка створюється директором ННІІТ. Оцінка комісії є остаточною. У випадку отримання студентом 0 балів (не зараховано), що постає підставою для відрахування за невиконання навчального плану.

Оцінювання студентів здійснюється за накопичувальною 100-бальною системою, складається із двох основних частин та розподіляється у співвідношенні: 60 *(бали напрацьовані під час вивчення дисципліни – поточний контроль),* 40 *(підсумкове оцінювання - залік)*:

Форми контролю	Види навчальної роботи	Оцінювання
ПОТОЧНИЙ	Виконання практичних робіт	36 балів

КОНТРОЛЬ	Самостійна робота	24 бали
ПІДСУМКОВЕ ОЦІНЮВАННЯ	Залік	40 балів
Додаткова оцінка		
Види навчальної роботи		**Оцінювання**
Участь у наукових конференціях, підготовка наукових публікацій за тематикою освітньої компоненти:		
- тези доповіді фахового спрямування;		3 бали
- стаття у фаховому виданні;		5 балів
Проходження дистанційних курсів та отримання сертифікатів на платформах Udemy, Прометеус, Coursera, Codecademy за тематикою освітньої компоненти		5 балів
Максимальна кількість додаткових балів, які можуть бути зараховані здобувачу освіти - 10 балів.		

ПІДСУМКОВА ОЦІНКА ЗА ДИСЦИПЛІНУ			
Бали	**Критерії оцінювання**	**Рівень компетентності**	**Оцінка** */запис в екзаменаційній відомості*
90-100	Студент демонструє повні й міцні знання навчального матеріалу в обсязі, що відповідає робочій програмі дисципліни, правильно й обґрунтовано приймає необхідні рішення в різних нестандартних ситуаціях. Вміє реалізувати теоретичні положення дисципліни в практичних розрахунках, аналізувати та порівнювати дані об'єктів діяльності фахівця на основі набутих з даної та суміжних дисциплін знань та умінь. Знає сучасні технології та методи розрахунків з даної дисципліни. За час навчання при проведенні практичних занять, виконанні індивідуальних завдань проявив вміння самостійно вирішувати поставлені задачі, активно включатись в дискусії, може відстоювати власну позицію в питаннях та рішеннях, які розглядаються. Зменшення 100-бальної оцінки може бути пов'язане з недостатнім розкриттям питань, що стосується тем дисципліни, але виходить за рамки об'єму матеріалу, передбаченого робочою програмою, або студент проявляє невпевненість в тлумаченні теоретичних положень або складних завдань.	**Високий** Повністю забезпечує вимоги до знань, умінь і навичок, що викладені в робочій програмі дисципліни. Власні пропозиції студента в оцінках і вирішенні практичних задач підвищує його вміння використовувати знання, які він отримав при вивченні інших дисциплін, а також знання, набуті при самостійному поглибленому вивченні питань, за тематикою дисципліни, яка вивчається.	Відмінно / Зараховано (А)
82-89	Студент демонструє гарні знання, добре володіє матеріалом, що відповідає робочій програмі дисципліни, робить на їх основі аналіз можливих ситуацій та вміє застосовувати теоретичні положення при вирішенні практичних задач, але допускає окремі неточності. Вміє самостійно виправляти допущені помилки, кількість яких є незначною. Знає сучасні технології та методи розрахунків з даної дисципліни. За час навчання при проведенні практичних занять, виконанні індивідуальних завдань та поясненні прийнятих рішень, дає вичерпні пояснення.	**Достатній** Забезпечує студенту самостійне вирішення основних практичних задач в умовах, коли вихідні дані в них змінюються порівняно з прикладами, що розглянуті при вивченні дисципліни	Добре / Зараховано (В)
75-81	Студент в загальному добре володіє матеріалом, знає основні положення матеріалу, що відповідає робочій програмі дисципліни, робить на їх основі аналіз можливих ситуацій та вміє застосовувати при вирішенні типових практичних завдань, але допускає окремі неточності. Вміє пояснити основні положення виконаних завдань та дати правильні відповіді при зміні	**Достатній** Конкретний рівень, за вивченим матеріалом робочої програми дисципліни. Додаткові питання про можливість використання	Добре / Зараховано (С)

	результату при заданій зміні вихідних параметрів. Помилки у відповідях / рішеннях / розрахунках не є системними. Знає характеристики основних положень, які мають визначальне значення при проведенні практичних занять, виконанні індивідуальних завдань та поясненні прийнятих рішень дисципліни, що вивчається.	теоретичних положень для практичного використання викликають утруднення.	
67-74	Студент засвоїв основний теоретичний матеріал, передбачений робочою програмою дисципліни, та розуміє постанову стандартних практичних завдань, має пропозиції щодо напрямку їх вирішень. Розуміє основні положення, що є визначальними в курсі, може вирішувати подібні завдання тим, що розглядались з викладачем, але допускає значну кількість незначних і грубих помилок, які може усувати за допомогою викладача.	**Середній** Забезпечує достатньо надійний рівень відтворення основних положень дисципліни	Задовільно / Зараховано (D)
60-66	Студент має певні знання, передбачені в робочій програмі дисципліни, володіє основними положеннями, що вивчаються на рівні, який визначається як мінімально допустимий. З використанням основних теоретичних положень, студент з труднощами пояснює правила вирішення практичних / розрахункових завдань дисципліни. Виконання практичних / індивідуальних завдань значно формалізовано: є відповідність алгоритму, але відсутнє глибоке розуміння роботи та взаємозв'язків з іншими дисциплінами.	**Середній** Є мінімально допустимим у всіх складових навчальної програми з дисципліни	Задовільно / Зараховано (E)
35-59	Студент може відтворити окремі фрагменти з курсу. Незважаючи на те, що програму навчальної дисципліни студент виконав, працював він пасивно, його відповіді під час практичних робіт в більшості є невірними, необґрунтованими. Цілісність розуміння матеріалу з дисципліни у студента відсутні.	**Низький** Не забезпечує практичної реалізації задач, що формуються при вивченні дисципліни	Незадовільно з можливістю повторного складання) / Не зараховано (FX) *В залікову книжку не проставляється*
0-34	Студент повністю не виконав вимог робочої програми навчальної дисципліни. Його знання на підсумкових етапах навчання є фрагментарними. Студент не допущений до здачі заліку.	**Незадовільний** Студент не підготовлений до самостійного вирішення задач, які окреслює мета та завдання дисципліни	Незадовільно з обов'язковим повторним вивченням / Не допущений (F) *В залікову книжку не проставляється*

ПОЛІТИКА ДОБРОЧЕСНОСТІ

Здобувач вищої освіти виконуючи самостійну або індивідуальну роботу повинен дотримуватись політики доброчесності. У разі наявності плагіату в будь-яких видах робіт Здобувача він отримує незадовільну оцінку і повинен повторно виконати завдання, які передбачені у Силабусі.