	Силабус навчальної дисципліни **«ТЕХНОЛОГІЯ ЗАХИСТ ІНФОРМАЦІЇ»** **Галузь знань: 12 «Інформаційні технології»** **Спеціальності: 122 «Комп'ютерні науки»** **Освітні програми: «Обслуговування програмних систем та комплексів»**
Статус дисципліни	Навчальна дисципліна є *нормативною*
Курс	4
Семестр	5
Обсяг дисципліни, кредити ЄКТС / загальна кількість годин	3 кредитів /90 год.
Мова викладання	**українська**
Що буде вивчатися (предмет навчання)	**Предметом** вивчення навчальної дисципліни є методи та технології захисту операційних систем, текстових редакторів, табличних процесорів, системи управління базами даних в локальних, корпоративних та глобальних комп'ютерних мережах банків та інших фінансових установ; на основі вивчених алгоритмів
Чому це цікаво / необхідно вивчити (мета) доступом	. Метою вивчення навчальної дисципліни «ТЕХНОЛОГІЯ ЗАХИСТУ ІНФОРМАЦІЇ» є – надання студентам комплексного розуміння технік, методів та стратегій, спрямованих на захист конфіденційної інформації в цифровому середовищі. Ця дисципліна орієнтована на ознайомлення з загрозами інформаційної безпеки, вивчення технологій криптографії, аутентифікації, контролю доступу, а також на засвоєння навичок управління інцидентами безпеки та відновлення після їх виникнення, сприяючи формуванню компетентності у сфері захисту даних та інформаційної безпеки в цілому;
Чому можна навчитись (компетентності)	Інтегральна компетентність Здатність вирішувати типові спеціалізовані задачі в галузі інформаційних технологій або у процесі навчання, що вимагає застосування положень і методів комп'ютерних наук та може характеризуватися певною невизначеністю умов; нести відповідальність за результати своєї діяльності; здійснювати контроль інших осіб у визначених ситуаціях. Загальні компетентності: ЗК5. Знання та розуміння предметної області та розуміння професійної діяльності ЗК8. Здатність вчитися і оволодівати сучасними знаннями Спеціальні компетентності СК2. Здатність використовувати теоретичні та фундаментальні знання в галузі комп'ютерних наук та інформаційних технологій для вирішення різноманітних проблем СК3. Здатність розробляти, аналізувати та застосовувати ефективні алгоритми для розв'язання конкретних професійних задач залежно від предметного середовища. СК4. Здатність здійснювати проєктування та розробку програмного забезпечення

	СК6. Здатність застосовувати методи та засоби захисту програмного забезпечення та даних від несанкціонованого доступу в умовах супроводження та експлуатації програмних систем і комплексів. Результати навчання: РН07. Застосовувати основні механізми та методи безпеки мереж і програмних систем
Як можна користуватись набутими знаннями і вміннями (результати навчання)	Знання з технологій захисту інформації можна застосовувати в сферах кібербезпеки, консультування, розробки ПЗ, аналізу ризиків, бізнес-аналітики, розробки політик безпеки, публікацій та інших областях, де важлива безпека даних.
Пререквізити	«Інформатика», «Математичні методи дослідження операцій»
Постреквізити	«Преддипломна практика»
Навчальна логістика	ЗМІСТОВИЙ МОДУЛЬ 1 . Основи захисту інформації Тема 1 Вступ. Законодавство України в сфері захисту інформації. Тема 2 Криптографія та її застосування. Основні принципи криптографії. Техніки шифрування та дешифрування. Використання криптографії для захисту даних ЗМІСТОВИЙ МОДУЛЬ 2 . Загрози та вразливості Тема 1 Комп'ютерні віруси, вразливості та атаки. Типи комп'ютерних вірусів та їх функції Тема 2 Безпека мереж та захист мережевої інфраструктури ЗМІСТОВИЙ МОДУЛЬ 3. Управління доступом та контроль ідентифікації Тема 1 Методи аутентифікації та авторизації. Принципи та методи перевірки ідентичності користувачів Тема 2 Контроль доступу до інформації. Методи контролю доступу до даних ЗМІСТОВИЙ МОДУЛЬ 4. Аспекти захисту в конкретних середовищах Тема 1 Захист персональних даних. Принципи етичного використання персональних даних Тема 2 Захист даних у веб-середовищі ЗМІСТОВИЙ МОДУЛЬ 5. Інциденти та відновлення Тема 1 Управління інцидентами та відновлення після порушень Тема 2 Безпека мобільних та хмарних технологій ЗМІСТОВИЙ МОДУЛЬ 6. Етика та законодавство Тема 1 Етичні аспекти та відповідальність у сфері захисту інформації Тема 2 Правові аспекти захисту інформації

Інформаційне забезпечення	**Рекомендована література** 1. . Тарнавський Ю. А. Технології захисту інформації: підручник / Ю.А. Тарнавський. – Київ: КПІ ім. Ігоря Сікорського, 2018. 162 с. 2. Технології захисту інформації: навч. посібник / С. Е. Остапов, С. П. Євсеєв, О. Г. Король. – Харків: Вид. ХНЕУ, 2018. 476 с. 3. Krasilenko V.G. Simulating and research of block parametric matrix affine-permutation ciphers (BP_MAPCs) for cryptographic transformations / V.G. Krasilenko, A.A. Lazarev, D.V. Nikitovich // тези доповідей П'ятнадцятої міжнародної науково-практичної конференції "Математичне та імітаційне моделювання систем. МОДС 2020", м. Чернігів, 29 червня – 01 липня 2020 р. – Чернігів: ЧНТУ, 2020. С. 123-128 Режим доступу: https://drive.google.com/file/d/1yj_eIMbJtoA1z5r_Q9SW7iNm_5PjYTrm/view

Політика навчальної дисципліни, оцінювання результатів навчання та академічна доброчесність	***Політика щодо відвідування та проведення занять***. Під час лекцій, практичних та лабораторних занять використовуються різноманітні інтерактивні технології навчання, які допомагають не тільки засвоїти теми курсу, а й розвинути навички критичного мислення, уміння працювати з інформацією, презентувати результати власних досліджень. Передбачається обов'язкова присутність студента на кожному занятті, тому що для отримання ефекту занурення у проблематику дисципліни необхідне групове обговорення певних завдань та шляхи їх вирішення («мозковий штурм»). Слід відзначити, що через відсутність студента на занятті можна втратити логіку опанування теоретичного та практичного матеріалу, якою пов'язані всі теми курсу. Як правило, викладач попереджає це на вступній лекції, на який відбувається знайомство зі структурно-логічною схемою курсу. У випадку, якщо була поважна причина відсутності студента на занятті, необхідно відвідати консультацію та з викладачем обговорити проблемні питання теми або низки тем через розбір «скрізних» питань, виконати практичні завдання. Під час вивчення курсу можна використовувати як рекомендовану літературу, так й різні інформаційні ресурси. Викладач контролює якість інформації, яку використовують здобувачі під час виконання завдань, вчить їх працювати з науковою інформацією, формує навички відрізняти якісну інформацію від неякісної. Мобільні пристрої під час проведення занять дозволяється використовувати лише для навчальних та наукових цілей. ***Політика щодо академічної доброчесності***. Політика щодо академічної доброчесності побудована на основі Положення про академічну доброчесність в ВСП «ФКЗІ ДУІТЗ». Усі види письмових робіт повинні бути написані здобувачами самостійно та мати високий рівень оригінальності. До заліку допускаються здобувачі, які виконали індивідуальне завдання. Здобувач, який не з'явився на залік або не був допущений на момент його проведення, має право повторно його пройти у визначені викладачем терміни під час консультацій/ відпрацювань. ***Загальна оцінка з дисципліни*** – максимум 100 балів. У випадку отримання менше 60 балів, здобувач обов'язково здійснює перескладання для ліквідації академічної заборгованості.
Локація та	***Навчальна аудиторія*** (дошка, проектор, ноутбук, інше

<table>
<tr><td>матеріально-технічне забезпечення</td><td colspan="2">обладнання).
Дистанційна – сучасні платформи та онлайн-сервіси дистанційного навчання.</td></tr>
<tr><td>Семестровий контроль</td><td colspan="2">залік</td></tr>
<tr><td>Циклова комісія</td><td colspan="2">інформаційних технологій</td></tr>
<tr><td rowspan="3">Викладач</td><td rowspan="3">  </td><td>ПІБ Орлова Лілія Борисівна</td></tr>
<tr><td>викладач вищої категорії, старший викладач</td></tr>
<tr><td>E-mail: orlovaliliia.fkzi@gmail.com</td></tr>
</table>