



Силабус навчальної дисципліни
«Основи і стандарти інформаційної безпеки»

Галузь знань: **12 «Інформаційні технології»**

Спеціальності: **122 «Комп'ютерні науки»**

Освітні програми: **«Обслуговування програмних систем та комплексів»**

Статус дисципліни	Навчальна дисципліна є <i>вибірковою</i>
Курс	3
Семестр	5
Обсяг дисципліни, кредити ЄКТС / загальна кількість годин	4 кредитів /120 год.
Мова викладання	українська
Що буде вивчатися (предмет навчання)	У курсі "Основи і стандарти інформаційної безпеки" студенти занурюються у концепції та ключові аспекти забезпечення безпеки інформації в сучасному цифровому світі. Це включає вивчення основних принципів кібербезпеки, аналіз потенційних загроз та ризиків, а також засоби їхнього запобігання. Студенти ознайомляються з міжнародними та національними стандартами інформаційної безпеки, такими як ISO/IEC 27001, які визначають основні вимоги до систем управління інформаційною безпекою. Досліджуються методи захисту конфіденційності, цілісності та доступності даних, принципи криптографії, політики безпеки, а також практичні аспекти впровадження та аудитування систем безпеки. Курс спрямований на надання студентам фундаментальних знань та інструментів для розуміння, планування та застосування ефективних стратегій інформаційної безпеки у сфері ІТ.
Чому це цікаво / необхідно вивчити (мета) доступом	Основи і стандарти інформаційної безпеки цікаво та актуально в контексті сучасного цифрового світу, оскільки ця сфера набуває все більшої важливості. Розуміння та володіння цими аспектами дозволяють розробникам, аналітикам та фахівцям з ІТ розуміти основні принципи захисту інформації та ефективно застосовувати їх у реальному житті. Це стає невід'ємною частиною будь-якої сучасної ІТ-кар'єри, відкриваючи можливості для працевлаштування в сферах кібербезпеки, аудиту, консультування та розробки програмного забезпечення. Отримані знання стають важливими для вирішення актуальних завдань захисту інформації та реагування на кіберзагрози, роблячи цей курс цікавим та важливим у сучасній ІТ-індустрії.

<p>Чому можна навчитись (компетентності)</p>	<p>Інтегральна компетентність</p> <p>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.</p> <p>Загальні компетентності:</p> <p>ЗК1. Здатність реалізувати свої права і обов'язки як члена суспільства, усвідомлювати цінності громадянського (вільного демократичного) суспільства та необхідність його сталого розвитку, верховенства права, прав і свобод людини і громадянина в Україні.</p> <p>ЗК2. Здатність зберігати та примножувати моральні, культурні, наукові цінності і досягнення суспільства на основі розуміння історії та закономірностей розвитку предметної області, її місця у загальній системі знань про природу і суспільство та у розвитку суспільства, техніки і технологій, використовувати різні види та форми рухової активності для активного відпочинку та ведення здорового способу життя.</p> <p>ЗК3. Здатність до абстрактного мислення, аналізу та синтезу.</p> <p>ЗК5. Знання та розуміння предметної області та розуміння професійної діяльності</p> <p>ЗК8. Здатність вчитися і оволодівати сучасними знаннями</p> <p>Спеціальні (фахові, предметні) компетентності:</p> <p>СК2. Здатність використовувати теоретичні та фундаментальні знання в галузі комп'ютерних наук та інформаційних технологій для вирішення різноманітних проблем.</p> <p>СК6. Здатність застосовувати методи та засоби захисту програмного забезпечення та даних від несанкціонованого доступу в умовах супроводження та експлуатації програмних систем і комплексів.</p> <p>Результати навчання:</p> <p>РН07. Застосовувати основні механізми та методи безпеки мереж і програмних систем.</p> <p>РН15. Розробляти супровідну документацію на різних етапах процесу життєвого циклу розробки програмного забезпечення</p>
<p>Як можна користуватись набутими знаннями і вміннями (результати навчання)</p>	<p>Набуті знання і вміння з інформаційної безпеки можна використовувати на різних рівнях. Наприклад, вони дозволяють розробляти та впроваджувати стратегії захисту даних у програмні продукти, забезпечуючи їхню конфіденційність та безпеку. Також ці знання корисні при аудиті систем безпеки, допомагаючи ідентифікувати потенційні вразливості та розробляти ефективні заходи їхнього запобігання. Безпека даних стає ключовим аспектом у будь-якій організації, тому знання з цієї області можуть бути використані у широкому спектрі професій, від розробки програмного забезпечення до управління системами безпеки в компаніях. Також вони дають змогу розуміти й аналізувати сучасні загрози та ризики, що дозволяє ефективніше реагувати на потенційні кібератаки та захищати цифрові ресурси.</p>
<p>Пререквізити</p>	<p>«Основи телекомунікацій та комп'ютерні мережі»</p>

Постреквізити	«Технологія захисту інформації»
Навчальна логістика	Звичайні теми лекцій з інформаційної безпеки: Основи кібербезпеки Стандарти інформаційної безпеки Криптографія та шифрування Захист мереж і систем Управління доступом та ідентифікація Безпека програмного забезпечення Стратегії відновлення після інцидентів
Політика навчальної дисципліни, оцінювання результатів навчання та академічна доброчесність	<p>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.</p> <p>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»).</p> <p>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 якій відбувається знайомство зі структурно-логічною схемою курсу.</p> <p>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.</p> <p>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.</p> <p>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.</p> <p>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.</p> <p>Загальна оцінка з дисципліни – максимум 100 балів. У випадку отримання менше 60 балів, здобувач обов'язково здійснює перескладання для ліквідації академічної заборгованості.</p>
Локація та	Навчальна аудиторія (дошка, проектор, ноутбук, інше)

матеріально-технічне забезпечення	обладнання). <i>Дистанційна</i> – сучасні платформи та онлайн-сервіси дистанційного навчання.
Семестровий контроль	<i>залік</i>
Циклова комісія	інформаційних технологій