АНОТАЦІЯ НАВЧАЛЬНОЇ ДИСЦИПЛІНИ

	ДИСЦИПЛІНА «Основи кібербезпеки та захисту інформаці» вільного вибору інституту
Спеціальності:	121 «Інженерія програмного забезпечення ня»;123 «Комп'ютерна інженерія»; 126 «Інформаційні системи і техно- логії»;151 «Автоматизація та компютерно-інтегровані технології»; 152 «Метрологія та інформаційно-вимірю- вальна техніка»
Мова викладання:	Українська
Кількість студентів, які можуть одночасно навчатися (мінімальна - максимальна):	10-30
Семестр, в якому викладається:	3-й курс, 5-й семестр
Кількість: кредитів ЄКТС академічних годин (вказати окремо лекції, лабораторні заняття, практичні заняття, самостійна робота тощо)	 3 90 годин (12 лекцій, 12 лабораторних, 66 самостійних)
Форма підсумкового контролю та наявність індивідуальних завдань:	диференційований залік
Кафедра, що забезпечує викладання:	Інформаційно-телекомунікаційний технологій та систем
Викладач, що планується для викладання (окремо по видах навантаження):	Воропаєва А.О., к.т.н., доц. (лек) Воропаєва А.О. к.т.н., доц. (лаб)
Попередні вимоги для вивчення дисципліни (якщо доречно):	немає
Перелік компетентностей, яких набуде студент після опанування даної дисципліни:	**Загальні:** Навички використання інформаційних і комунікаційних технологій. **Фахові:** Здатність використовувати сучасні інформаційні системи та технології (виробничі, підтримки прийняття рішень, інтелектуального аналізу даних та інші), методики й техніки кібербезпеки під час виконання функціональних завдань та обов'язків. Здатність аналізувати, вибирати і застосовувати методи і засоби для забезпечення інформаційної безпеки (в тому числі кібербезпеки). Здатність забезпечувати захист інформації, що обробляється в комп'ютерних та кіберфізичних системах та мережах з метою реалізації встановленої політики інформаційної безпеки **Результати навчання:**

	Створювати високонадійні системи автоматизації з високим рівнем функціональної та інформаційної безпеки програмних та технічних засобів. Знати, аналізувати, вибирати, кваліфіковано застосовувати засоби забезпечення інформаційної безпеки (в тому числі кібербезпеки) і цілісності даних відповідно до розв'язуваних прикладних завдань та створюваних програмних систем.
Сфера реалізації компетентностей в майбутній професії:	Сучасний спеціаліст в галузі інформаційних технологій має дотримуватись правил поводження з інформацією у кіберсфері та безпечної роботи із засобами комп'ютерної техніки та володіти наступними вміннями: визначати заходи кібербезпеки для конкретної ситуації; оцінювати загрози та вживати заходів реагування на робочому місці; безпечно поводитись у кіберсфері; організовувати безпечний доступ до пристроїв і програм; критично оцінювати інформацію.
Особливості навчання на курсі:	Практично-орієнтована дисципліна. Для забезпечення перелічених компетентностей використовуються матеріали мережевої академії Cisco (курс вступ до кібербезпеки).
Матеріально-технічне забезпечення:	1) комп'ютерна техніка; 2) доступ до Інтернет.
Лінк на дисципліну:	https://drive.google.com/drive/folders/1WYhye3u2xUqBQNklzVmSKITiMIg7cax1?usp=sharing посилання на основні матеріали курсу www.netacad.com посилання на мережеву академію Cisco
Стислий опис дисципліни:	Загальні правила безпечної роботи з пристроями та програмами. Безпека мобільних пристроїв. Шкідливе програмне забезпечення. Фізична безпека. Убезпечення від неправдивих повідомлень. Базові правила убезпечення роботи в комп'ютерній мережі. Соціальна інженерія. Безпечне користування мережею Інтернет. Безпечне користування електронною поштою. Безпека користування соціальними мережами Класифікація видів загроз в інформаційному просторі. Шляхи розповсюдження загроз кібербезпеки. Три виміри куба кібербезпеки. Стани даних. Засоби протидії кіберзлочинності. Структура керування ІТ-безпекою. Шкідливе програмне забезпечення та зловмисний код. Типи кібератак. Атаки на безпроводові мережі та мобільні пристрої. Криптографія. Контроль доступу. приховування даних. Типи засобів контролю цілісності даних. Цифровий підпис. Цифровий сертифікат. Забезпечення цілісності баз даних. Висока доступність. Засоби для поліпшення доступності. реагування на інциденти. Захист систем та пристроїв. Укріплення захисту серверів. Укріплення захисту мережі.