ДЕРЖАВНИЙ ТОРГОВЕЛЬНО-ЕКОНОМІЧНИЙ УНІВЕРСИТЕТ
СИСТЕМА УПРАВЛІННЯ ЯКІСТЮ
Система забезпечення якості освітньої діяльності та якості вищої освіти
сертифікована на відповідність ДСТУ ISO 9001:2015 / ISO 9001:2015
Кафедра інженерії програмного забезпечення та кібербезпеки

СИЛАБУС

ОСНОВИ КІБЕРБЕЗПЕКИ / CYBERSECURITY ESSENTIALS

SYLLABUS

освітній ступінь	**бакалавр /** bachelor
галузь знань	**12 Інформаційні технології /** Information Technology
спеціальність	**121 Інженерія програмного забезпечення /** Software Engineering
освітня програма	**Інженерія програмного забезпечення /** Software Engineering

Київ 2023

Викладач: Костюк Юлія Володимирівна,

вчене звання та посада: старший викладач кафедри інженерії програмного забезпечення та кібербезпеки;

контактний телефон: (044)-531-49-57;

e-mail: kostyuk_yu@knute.edu.ua

наукові інтереси: комп'ютерні мережі, інформаційно-інтелектуальні системи, хмарні технології, кібербезпека

1. Дисципліна: «ОСНОВИ КІБЕРБЕЗПЕКИ»,

- рік навчання: I-IV;
- семестр навчання: 2-8;
- кількість кредитів: 6;
- *кількість годин за семестр: 180 год.*
  - лекційних: *24 год.*
  - лабораторних: *24 год.*
  - на самостійне опрацювання: *132 год.*
- *кількість аудиторних годин на тиждень:*
  - лекційних: *2 год.*
  - лабораторних: *2 год*.

2. Час та місце проведення:

- *аудиторні заняття* - відповідно до розкладу ДТЕУ з врахуванням специфіки дисципліни проведення останньої передбачено в аудиторіях: 505, 510, 514;
- *поза аудиторна робота* - самостійна робота студента, результат виконання якої висвітлено засобами Office 365;
- *всі лабораторні завдання виконуються* на основі інтерактивних методів навчання у електронному середовищі. Передбачається можливість проведення лабораторних та лекційних занять на базах підприємств-партнерів.

3. Пререквізити та постреквізити навчальної дисципліни:

- **пререквізити:** дисципліна базується на знаннях та компетентностях, що набуває здобувач вищої освіти під час вивчення дисциплін «Основи інженерії програмного забезпечення», «Організація комп’терних мереж».

– **постреквізити:** дисципліна надає студентам необхідні знання та навички, які будуть корисні при вивченні дисциплін «Моделювання та аналіз програмного забезпечення», «Програмування Інтернет», «Технології розробки та тестування програмного забезпечення», при проходженні практичної підготовки, підготовки та захисту кваліфікаційної роботи, у подальшій професійній діяльності.

Програмні результатів навчання:

ПР21	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.
ПР25	Розуміти і реалізувати свої права і обов'язки як члена суспільства, усвідомлювати цінності вільного демократичного суспільства, верховенства права, прав і свобод людини і громадянина в Україні.
ПР26	Діяти на основі законодавчої та нормативно-правової бази України та вимог відповідних стандартів, у тому числі міжна¬родних в галузі інформаційної та /або кібербезпеки.

4. Характеристика дисципліни:

4.1. Призначення навчальної дисципліни: дисципліна «Основи кібербезпеки» є важливою складовою підготовки сучасних фахівців з розробки інформаційних технологій. Її місце – на перетині традиційних фундаментальних дисциплін та дисциплін професійної підготовки бакалаврів.

4.2.Мета вивчення дисципліни: формування у майбутніх фахівців необхідного рівня знань щодо правильного поводження з інформацією у кіберсфері та безпечної роботи із засобами комп'ютерної техніки в професійній діяльності. дізнатись про основні загрози в сучасному інформаційному просторі; аналізувати поширені помилки користувачів та наслідки від атак зловмисників і кібершахраїв; вивчити базові правила захисту інформації на персональних електронних пристроях та в соціальних мережах; навчитись визначати фейкові новини; опанувати основні рекомендації щодо захисту власних даних, безпечного користування електронними пристроями та інформаційними ресурсами.

4.3.Задачі вивчення дисципліни: знання основних положень, термінів та заходів, що стосуються кібергігієни на робочу місці; знання основної нормативно-правової бази у сфері кібербезпеки та інформаційної безпеки; знання особливостей кібергігієни в системі публічної служби, уміння визначати заходи кібергігієни для конкретної ситуації; уміння оцінювати загрози та вживати заходів реагування на робочому місці; уміння безпечно поводитись у кіберсфері, навички організації безпечного доступу до пристроїв і програм; навички правильного налаштування програмного забезпечення на робочому місці; навички критичного оцінювання інформації; знати різні типи

зловмисного ПЗ (відомого як шкідливі програми) та їх симптоми; знати різні методи, якими нападники можуть проникнути в систему: соціальна інженерія, злам паролю Wi-Fi, фішинг та використання вразливостей.

Загальні компетентності:

К02	Здатність застосовувати знання у практичних ситуаціях.
К05	Здатність вчитися і оволодівати сучасними знаннями.
К13	Здатність здійснювати професійну діяльність у відповідності з чинними нормативними та правовими актами.

Спеціальні (фахові, предметні) компетентності:

К19	Здатність аналізувати, вибирати і застосовувати методи і засоби для забезпечення інформаційної безпеки (в тому числі кібербезпеки).
К21	Здатність застосовувати фундаментальні і міждисциплінарні знання для успішного розв'язання завдань інженерії програмного забезпечення.

4.4. Зміст навчальної дисципліни: відповідає навчальній та робочій програмі, яка відповідає запитам стейкхолдерів.

5. План вивчення дисципліни:

ТЕОРЕТИЧНИЙ БЛОК:

Навчальна діяльність	**Робочий час студента (год.)**
1	2
Лекція №1 ***Кіберпростір і кібербезпека — головні ознаки нової інформаційної цивілізації.*** *План лекції №1* 1. Поняття інформаційна безпека, кібербезпека, кіберпростір, кібероборотьба, кібертероризм, кіберзброя**.** 2. Кіберпростір: визначення, система відношень, загрози. Потреба в кібербезпеці. 3. Кіберінциденти: передумови скоєння та наслідки. 4. Поняття «кібервійни». Захист даних та конфіденційності. 5. Огляд областей кібербезпеки. Приклади доменів кібербезпеки. 6. Поняття «кіберзлочинець» та мотиви кіберзлочинів. Класифікація зловмисників. **Список рекомендованих джерел:** *Основний: 1[с. 50-59, 66-98, 257-268, 310-312], 2 [с. 7-43], 3 [с. 27-38, 130-146], 4 [с. 112-120].* *Додатковий: 6 [с. 25-28, 172-176, 239, 249-252, 255-263].* *Інтернет-ресурси: 14.*	1
Лекція №2 Національна система кібербезпеки України План лекції №2 1. Національна безпека України: реалії та перспективи. Роль та місце кібернетичної безпеки у загальній системі нацбезпеки. 2. Основні положення Стратегії кібербезпеки України.	1

1	2
3. Компетенція органів державної влади, органів місцевого самоврядування та їх посадових осіб у сфері охорони державної таємниці. 4. Правове забезпечення у сфері інформаційної безпеки та кібербезпеки. Список рекомендованих джерел: Основний: 1 [с. 135-149], 2 [с. 7-24], 3 [с. 222-240], 4 [с. 137-138]. Додатковий: 6 [с. 189-209], 7 [с. 93-106], 10, 11, 12. Інтернет-ресурси: 14, 16.	
Лекція 3. Сутність та основні процедури керування кібербезпекою План лекції №3 1. Модель кібербезпеки ISO. 2. Куб кібербезпеки. 2. Захист конфіденційності даних. Керування доступом. 3. Потреба в цілісності даних. Перевірка цілісності. 4. Принцип доступності. П'ять дев'яток. Забезпечення доступності. 5. Проблеми захисту збережених даних. Методи передачі даних. Проблеми захисту даних у процесі обробці. Список рекомендованих джерел: Основний: 1 [с. 54-59], 3 [с. 157-166]. Додатковий: 6 [с. 218-219]. *Інтернет-ресурси: 14, 15, 16*	1
Лекція 4. ***Кібератаки, загрози та їх властивості. Характеристика сучасних кібератак*** *План лекції №4* 1. Сутність та класифікація кібератак. Етапи реалізації атак. 2. Атаки на бездротові мережі та мобільні пристрої. Атаки на WEP та WPA. 3. Атаки на застосунки. Міжсайтовий скриптинг. Ін'єкція коду. Переповнення буфера. Віддалений запуск програм. 4. Атака "Відмова в обслуговуванні" (DoS). Розподілена DoS атака (Distributed DoS Attack, DDoS). 5. Зміст, класифікація та ознаки кіберзагроз. Основні характеристики кіберзагроз. Поширення кіберзагроз. Кіберзагрози підвищеної складності. **Список рекомендованих джерел:** *Основний: 1 [с. 66-96, 168-179], 2 [с. 43-62], 3 [с. 92-138], 4 [с. 9-23].* *Додатковий: 6 [с. 296-299, 340-354], 8 [с. 50-82, 197-201].* *Інтернет-ресурси: 14, 15..*	1
Лекція 5. ***Дезінформація як елемент кібератак. Сценарії розвитку та методи протидії*** *План лекції №5* 1. Канали поширення дезінформації. Типи неправдивої інформації. 2. Технології неправдивих повідомлень. Інструменти виявлення неправдивих повідомлень. 3. Види маніпуляцій. Пропаганда як інструментів інформаційного впливу. 4.Маніпулювання новинами. Маніпулювання експертними оцінками. Маніпулювання повідомленнями. Маніпуляції з результатами досліджень. **Список рекомендованих джерел:** *Основний: 3 [с. 19, 43-60, 64-79], 4 [с. 97-102].* *Додатковий: 7 [с. 87-90].* *Інтернет-ресурси: 14, 15.*	2
Лекція №6	

1	2
Комп'ютерна вірусологія *План лекції №6* 1. Поняття про комп'ютерні віруси, історія їх виникнення та розвитку. Загальні принципи функціонування комп'ютерних вірусів, їх розмноження. Алгоритми роботи вірусів. 2. Класифікація комп'ютерних вірусів: файлові, завантажувальні (бутові) та файлово-завантажувальні віруси, макровіруси, мережні віруси. 3. Класифікаційний код вірусу. Резидентність, використання стелсалгоритмів, самошифрування та поліморфізм, використання нестандартних методів. 4. Шкідливе програмне забезпечення (ШПЗ). Шляхи розповсюдження ШПЗ, вектори атак. Типи шкідливого програмного забезпечення. Симптоми зараження шкідливим ШПЗ. Шпигунські програми (spyware). 5. Завантажувач (дропер/лоадер). Викрадач інформації «інфостілер або стілер». Keylogger "кейлогер". «JS-сніфери». Троянські програми віддаленого доступу.rat. Банківські трояни (banking trojans). Ransomware (програма-вимагач, програма-шантажист). Майнери (miners). 6. Шкідливе програмне забезпечення для знищення інформації без можливості її відновлення. 7. Рекламне шкідливе програмне забезпечення (adware). **Список рекомендованих джерел:** *Основний: 3 [с. 170-211].* *Додатковий: 7 [с. 69-96].* *Інтернет-ресурси: 14, 15*	2
Лекція 7. ***Соціальна інженерія*** ***План лекції №7*** 1. Поняття соціальної інженерії. Методи соціальної інженерії. 2. Види атак соціальної інженерії. Претекстінг (pretexting). Тейлгейтінг (tailgating). Послуга за послугу (quid pro quo). Злам пароля WI-FI. Атаки грубої сили (brute-force attacks). Прослуховування мережі (network sniffing). 3. Фішингова атака. 4. Етапи атаки із використанням СІ (соціальної інженерії). Легендування та планування атаки із використання методів СІ. 5. Використання вразливостей як розповсюджений метод проникнення для отримання інформації **Список рекомендованих джерел**: *Основний: 2 [с. 112-148], 3 [с. 83-91].* *Додатковий: 6 [с. 136-140], 7 [с. 8-25].* *Інтернет-ресурси: 14.*	2
Лекція 8. ***Соціотехнічна безпека: проблемні аспекти*** *План лекції №8* 1. Соціальна інженерія як метод розвідки складних соціальних і соціотехнічних систем, бізнес-проєктів в сфері креативних індустрій. 2. Особливості захисту сучасної інфосфери в умовах стороннього кібернетичного впливу. 3. Соціальний фактор у проблемі забезпечення інформаційної і кібербезпеки. 4. Соціальні мережі: особливості, основні поняття та визначення. Моніторинг соціальних мереж − цілі та способи реалізації. 5. Поняття соціотехнічної системи та її властивостей.	2

1	2
6. Системний підхід як загальнометодологічний принцип створення складних соціотехнічних систем. **Список рекомендованих джерел:** *Основний: 2 [с. 64-95].* *Додатковий: 6 [с. 144-159], 7 [с. 97-99].* *Інтернет-ресурси: 14*	
Лекція №9 ***Безпека спілкування в кіберпросторі*** ***План лекції №9*** 1. Захист інформації в глобальних мережах. 2. Характер проведення атак у глобальних мережах. 3. Безпечне користування мережею «Інтернет» під час успішного для успішного управління культурними проєктами, промисловому менеджменті та стартапами креативних індустрій (у сфері ІТ-технологій, арт-, івент-, медіа-, сфера дозвілля, дизайн, PR-бізнес, у сфері менеджменту, в професійній діяльності у сфері виробництва та управління якістю і безпечністю харчових продуктів, зокрема у сфері ресторанних технологій тощо); процесами їх комерціалізації та ефективного просування на національному та міжнародному ринках з використанням сучасних інформаційно-комунікаційних технологій. 4. Найпоширеніші способи нелегального заробітку в мережі «Інтернет». 5. Безпека браузерів. 6. Безпека даних під час успішного для успішного управління культурними проєктами, у сфері ІТ-технологій, стартапами креативних індустрій (арт-, івент-, медіа-, сфера дозвілля, дизайн, PR-бізнес, в професійній діяльності у сфері виробництва та управління якістю і безпечністю харчових продуктів, зокрема у сфері ресторанних технологій тощо); процесами їх комерціалізації та ефективного просування на національному та міжнародному ринках з використанням сучасних інформаційно-комунікаційних технологій. 7. Безпечне користування мережами WI-FI. Основні правила безпечного користування WI-FI. 8. Безпечне користування месенджерами. **Список рекомендованих джерел:** *Основний: 2 [с. 24-43].* *Додатковий: 6 [с. 495-508], 7 [с. 41-52].* *Інтернет-ресурси: 14*	2
Лекція 10. ***Особливості економічної діяльності суб'єктів господарювання в кіберпросторі*** *План лекції №10* 1. Безпека користування соціальними мережами. Реєстрація. Стійкий пароль. Оновлення паролів та парольних фраз. 2. Конфіденційність даних. Налаштування конфіденційності та інших питань безпеки. 3. Безпека мобільних пристроїв. Блокування доступу до пристрою. Безпечна робота в мультимедійних засобах спілкування. Передавання вживаних мобільних пристроїв іншим особам. Передавання контактної інформації іншим особам. Вірусне програмне забезпечення. Додаткові функції мобільного пристрою. Головні правила роботи з мобільними пристроями. 4. Безпека користування електронною поштою. Конфіденційність електронної пошти. Найвідоміші атаки через електронну пошту. Загрози під час	2

1	2
користування поштовою скринькою. Легітимні та фішингові листи (investigation). 5. Забезпечення безпеки особистої поштової скриньки (рекомендації). **Список рекомендованих джерел:** *Основний: 2 [с. 130-147], 4[с. 35-49, 68-70].* *Додатковий: 7 [с. 55-67, 97-99, 105-123].* *Інтернет-ресурси: 14*	
Лекція №11 **Безпека цифрового простору суб'єктів господарювання** *План лекції №11* **1.** Технічні канали витоку інформації. Способи несанкціонованого зняття інформації з технічних каналів її витоку. **2.** Класифікація каналів витоку інформації. Методи блокування технічних каналів витоку інформації. **3.** Системи та засоби виявлення, пошуку та знешкоджування технічних засобів зняття інформації. **4.** Захист акустичної інформації від зняття радіопристроями. **5.** Захист інформації від витоку по технічних каналах, утворених допоміжними технічними засобами. **6.** Захист інформації від несанкціонованого запису звукозаписувальними пристроями. **7.** Захист електронної інформації. **8.** Захист письмової інформації від оптичного зняття. **Список рекомендованих джерел:** *Основний: 2 [с. 151-181], 3 [с. 43-60, 290-305].* *Додатковий: 7 [с. 123-127].* *Інтернет-ресурси: 14*	2
Лекція 12. ***Безпека Інтернету-речей*** *План лекції №12* 1. Історія Інтернету-речей. Екосистема Інтернету-речей. 2. Архітектура Інтернету-речей. Технології Інтернету-речей. «Розумний та безпечний будинок». 3. Анатомія кібератак на IoT-пристрої. Mirai. Stuxnet. Ланцюжкова реакція. Туманні технології. 4. Криптографія. Симетрична криптографія. Асиметрична криптографія. 5. Криптографічний хеш (аутентифікація і цифровий підпис). 6. Інфраструктура відкритого ключа. 7. Блокчейн і криптовалюта в Інтернеті-речей. 8. Рекомендації щодо захисту IoT-пристроїв. **Список рекомендованих джерел:** *Основний: 2 [с. 163-167].* *Додатковий: 6 [с. 398-404, 480-482], 9 [с. 15-18, 111-127, 159-170, 189-200].* *Інтернет-ресурси: 14*	2
Лекція 13. ***Системи захисту інформації на проникнення*** *План лекції №13* 1. Технології захисту на основі програмного забезпечення. Апаратні засоби захисту. Мережні технології захисту. Хмарні технології захисту. 2. Фізична безпека. Загрози, пов'язані з недотриманням правил фізичної безпеки. Найпопулярніша атака через фізичне втручання: Stuxnet. 3. Захист інформації за допомогою міжмережних екранів (брандмауера).	2

1	2
4. Маскування даних. Технології маскування даних. Стеганографія, основні терміни та визначення. Методи та моделі стеганографії. Комп'ютерна і цифрова стеганографія, цифрові водяні позначки. 5. Практичні аспекти побудови стеганосистем. Приховування даних у текстових файлах: методи текстової стеганографії; аналіз реалізації методів. **Список рекомендованих джерел:** *Основний: 1 [с. 188-205], 2 [с. 158-159], 3 [с. 290-312].* *Додатковий: 7 [с. 123-127].* *Інтернет-ресурси: 14*	
Лекція №14 ***Основні методи забезпечення кібербезпеки суб'єкта господарювання*** *План лекції №14* **1.** Типи контролю доступу. **2.** Стратегії контролю доступу. Дискреційне розмежування доступу. Контроль доступу на основі ролей. Розмежування доступу на основі правил. **3.** Ідентифікація. Методи аутентифікації. Багатофакторна аутентифікація. Аутентифікація на основі одноразових паролей. Строга аутентифікація. Криптографічні протоколи строгої аутентифікації. Біометрична аутентифікація користувача. Використання авторизації. **4.** Типи засобів контролю безпеки. Превентивні засоби контролю. Стримуючі засоби контролю. Коригуючі засоби контролю. Засоби відновлення. Компенсуючі засоби контролю. **5.** Криптографія і її основні поняття. Модель криптографічної системи. Принцип Керкхоффса. Етапи розвитку криптографічних систем. Види історичних шифрів. **6.** Типи шифрування. Шифрування за допомогою закритого ключа. Процес симетричного шифрування. Типи криптографічних перетворень. Симетричні криптосистеми шифрування. Алгоритм шифрування DES, 3-DES. Стандарт шифрування AES. Основні режими роботи блочного симетричного алгоритму. **Список рекомендованих джерел:** *Основний: 1 [с. 188-193, 205-210], 3 [с. 318-348].* *Додатковий: 6 [с. 398-411, 480-491].* *Інтернет-ресурси: 14*	2

ЛАБОРАТОРНІ ЗАНЯТТЯ

Навчальна діяльність	Робочий час студента (год.)	Оцінювання (бал)
1	2	3
Лабораторне заняття №1 **Кібернетичний простір та доступ до системи WWW за допомогою веб-браузера** Мета: 1) поглиблення та закріплення теоретичних знань з наступних питань: - кібернетичний простір: термінологія, структура; - поява та розвиток Інтернет; - основні поняття системи WWW; - структура верхнього рівня веб-браузера.	1	5

1	2	3
2) набуття практичних навичок роботи з веб-браузерам та використанння їх для успішного управління культурними проєктами та стартапами креативних індустрій та промисловому менеджменті (у сфері ІТ-технологій, арт-, івент-, медіа, сфера дозвілля, дизайн, PR-бізнес, у сфері менеджменту, в професійній діяльності у сфері виробництва та управління якістю і безпечністю харчових продуктів, зокрема у сфері ресторанних технологій тощо). Завдання: 1) виконати теоретичне завдання згідно з номером варіанту, який приведено в табл. 1., особливо звернути увагу на механізми забезпечення інформаційної безпеки в веб-браузерах. 2) Знайти і обробити інформацію відповідно до завдання та підготувати коротку доповідь (міні-презентацію). 3) провести порівняльний аналіз 2-3 обраних браузерів та сформувати відповідну порівняльну таблицю щодо забезпечення інформаційної безпеки. 4). Оформити звіт згідно до вимог (додаток 1). 5). Зробити висновки, відповісти письмово на контрольні питання та підготуватися до усного опитування.		
Лабораторне заняття №2 **Інформаційна безпека держави. Потенційні загрози, засоби їх попередження та ліквідації** **Мета:** ознайомитися з поняттям інформаційної безпеки держави та інформаційної війни, основними інтересами України та потенційними небезпеками у сфері інформаційної безпеки, елементами інформаційної боротьби; законодавством України, що стосується інформаційної безпеки держави для успішного управління процесами їх комерціалізації та ефективного просування. **Завдання:** 1) Користуючись однією з пошуковх систем (Google, чи будь-якою іншою) ознайомтеся із законодавчою базою України, що стосується інформаційної безпеки держави. Назви основних законів, указів президента, постанов, положень записати до звіту (не менше 10). 2) На офіційному сайті Верховної ради «Законодавство України» (http://zakon2.rada.gov.ua/laws) знайдіть Закон України «Про Основні засади розвитку інформаційного суспільства в Україні на 2007-2015 роки», ознайомтесь з його основними положеннями та занотуйте до звіту такі відомості: - основні стратегічні цілі розвитку інформаційного суспільства в Україні; - основні напрямки розвитку інформаційного суспільства в Україні; - законодавче забезпечення розвитку інформаційного суспільства; - інформаційна безпека в інформаційному суспільстві. 3) Користуючись однією з пошукових систем (Google, чи будь-якою іншою) знайдіть текст Доктрини інформаційної безпеки України, ознайомтесь з основними положеннями та занотуйте до звіту такі відомості: - основні напрями забезпечення державою національного інформаційного суверенітету; - принципи забезпечення інформаційної безпеки України; - основні реальні та потенційні загрози інформаційній безпеці України у сфері державної безпеки; - основні засади державної політики забезпечення інформаційної безпеки України; зробити висновки та письмово дати відповіді на питання.	1	5
Лабораторне заняття №3 **Ідентифікація загроз**	1	5

Мета: Вивчення можливостей забезпечення функцій безпеки, які використовуються організаціями для збереження даних для успішного управління культурними проєктами, промисловому менеджменті та стартапами креативних індустрій (у сфері IT-технологій, івент-, медіа-, сфера дозвілля, дизайн, PR-бізнес, у сфері менеджменту, в професійній діяльності у сфері виробництва та управління якістю і безпечністю харчових продуктів, зокрема у сфері ресторанних технологій тощо); процесами їх комерціалізації та ефективного просування на національному та міжнародному ринках з використанням сучасних інформаційно-комунікаційних технологій. Завдання: Дослідити загрози, що витікають від кібератак. Дослідити тріаду CIA (конфіденційність, цілісність і доступність) та типи кібератак.		
Лабораторне заняття №4 ***Візуалізація «чорних» хакерів*** **Мета:** Вивчити та проаналізувати інциденти кібербезпеки. **Завдання:** після дослідження та аналізу дати відповіді на запитання: Хто є хакером? До якої організації або групи належить хакер? Який мотив у хакера? Який метод атаки був використаний? Що було метою і в чому була вразливість, використана проти компанії? Як можна було запобігти цій атаці або зменшити її наслідки? Як це впливає на успішне управління культурними проєктами, промисловому менеджменті та стартапами креативних індустрій (у сфері IT-технологій, на основі застосування наукових і математичних принципів, арт-, івент-, медіа-, сфера дозвілля, дизайн, PR-бізнес, у сфері менеджменту, в професійній діяльності у сфері виробництва та управління якістю і безпечністю харчових продуктів, зокрема у сфері ресторанних технологій тощо); процесами їх комерціалізації та ефективного просування на національному та міжнародному ринках з використанням сучасних інформаційно-комунікаційних технологій.	1	5
Лабораторне заняття №5 **Підвищення безпеки облікового запису Google** **Мета:** Захист особистих даних. Підвищення безпеки облікового запису Google. Краще зрозуміти заходи безпеки та сервіси, які такі організації, як Google, здійсняють для захисту інформації та інформаційних систем для успішного управління культурними проєктами, промисловому менеджменті та стартапами креативних індустрій (у сфері IT-технологій, на основі застосування наукових і математичних принципів, арт-, івент-, медіа-, сфера дозвілля, дизайн, PR-бізнес, у сфері менеджменту, в професійній діяльності у сфері виробництва та управління якістю і безпечністю харчових продуктів, зокрема у сфері ресторанних технологій тощо). **Завдання:** 1) Проаналізувати можливості функцій безпеки, які використовують такі організації, як Google та Cisco, для захисту даних. Дізнатися як Google гарантує, що сервери, які вони встановлюють у своїх центрах обробки даних (ЦОД), не заражені зловмисним програмним забезпеченням виробниками обладнання. 2) Визначення вразливостей даних. 3) Вміти захистити доступ до облікового запису	2	5
Лабораторне заняття №6 **Комп'ютерні віруси: знайомство з принципами роботи. Захист від вірусів. Огляд основних антивірусних програм** **Мета:** ознайомитись з основними видами комп'ютерних вірусів, принципами їх роботи поширення і знищення. Розглянути програми для	2	5

захисту від вірусів, принцип дії, ефективність, можливості для успішного управління процесами їх комерціалізації та ефективного просування на національному та міжнародному ринках з використанням сучасних інформаційно-комунікаційних технологій. **Завдання:** вибрати один з типів вірусів і описати його за планом: назви вірусів даного типу; принцип роботи даного типу вірусів; методи поширення даного типу вірусів; програми для знищення даного типу вірусів; методи для знищення даного типу вірусів. Оформити звіт по роботі та дати письмово відповідь на контрольні питання.		
Лабораторне заняття №7 **Хто володіє даними: правила надання послуг у сфері ІТ-технологій, на основі застосування наукових і математичних принципів, у сфері креативних індустрій (арт-, івент-, медіа-, сфера дозвілля, дизайн, PR-бізнес, в професійній діяльності у сфері виробництва та управління якістю і безпечністю харчових продуктів, зокрема у сфері ресторанних технологій тощо)** **Мета:** Дослідити яким є право власності на особисті дані, якщо вони зберігаються не в локальній системі. Ознайомитися з правилами надання послуг для успішного управління процесами їх комерціалізації та ефективного просування на національному та міжнародному ринках з використанням сучасних інформаційно-комунікаційних технологій **Завдання:** дослідити правові угоди, необхідні для використання різних онлайн-сервісів. Дізнатися про деякі способи захисту особистих даних.	2	5
Лабораторне заняття №8 **Інциденти порушення безпеки, несанкціонований доступ до даних в професійній діяльності у сфері ІТ-технологій, на основі застосування наукових і математичних принципів, у сфері виробництва та управління якістю і безпечністю харчових продуктів, зокрема у сфері ресторанних технологій, креативних індустрій** **Мета:** Знайти інформацію та прочитати про деякі нещодавні порушення безпеки; ознайомитись з декількома інцидентами порушення безпеки, щоб визначити, що було зроблено, які експлойти було використано, і що потрібно зробити, щоб захистити особисті дані. **Завдання:** Використовуючи три надані посилання, в яких описано порушення безпеки у різних секторах, заповнити таблицю. Знайти декілька додаткових цікавих випадків порушень кібербезпеки та зазначити їх у висновку в таблиці	2	5
Лабораторне заняття №9 **Захист комп'ютерних мереж та персональних комп'ютерів за допомогою брандмауера (Firewall)** **Мета:** ознайомитися з основним типами, призначенням, базовими функціями брандмауера, зробити загальний огляд вбудованого брандмауера операційної системи Windows під час успішного для успішного управління культурними проєктами, у сфері ІТ-технологій, на основі застосування наукових і математичних принципів здійснювати проектування, та підтримку комп'ютерного програмного забезпечення, використовуючи різні мови програмуванняпромисловому менеджменті та стартапами креативних індустрій (у сфері ІТ-технологій, арт-, івент-, медіа-, сфера дозвілля, дизайн, PR-бізнес, в професійній діяльності у сфері виробництва та управління якістю і безпечністю харчових продуктів, зокрема у сфері ресторанних технологій, у сфері менеджменту тощо); процесами їх комерціалізації та ефективного просування на	2	5

національному та міжнародному ринках з використанням сучасних інформаційно-комунікаційних технологій.		
Лабораторне заняття №10 ***Створення та збереження надійних паролів у сфері IT-технологій, креативних індустрій тощо*** **Мета:** Один із найважливіших способів захистити свої облікові записи в Інтернеті – захистити паролі**.** Зрозуміти концепцію надійного пароля. Необхідно мати різні паролі для різних служб. Часте оновлення паролів є обов'язковим. Рекомендується використання (не дуже розумних або ж навпаки улюблених) фраз як спосіб створення паролів. Потрібно завжди пам'ятати про використання двоетапної перевірки вашого пароля, у сфері IT-технологій, промисловому менеджменті та успішного управління культурними проєктами та стартапами креативних індустрій (арт-, івент-, медіа-, сфера дозвілля, дизайн, PR-бізнес, в професійній діяльності у сфері виробництва та управління якістю і безпечністю харчових продуктів, зокрема у сфері ресторанних технологій у сфері менеджменту тощо); процесами їх комерціалізації та ефективного просування на національному та міжнародному ринках з використанням сучасних інформаційно-комунікаційних технологій**.** **Завдання:** Дослідження концепцій створення надійного пароля: створення надійного пароля. Дослідження концепцій безпечного збереження паролів: безпечне зберігання паролів. Використовуючи характеристики надійного пароля, вибрати пароль, який легко запам'ятати, але важко вгадати. Використати для зберігання паролей менеджер паролів.	2	4
Лабораторне заняття №11 ***Перевірка факту компрометації поштової адреси. Двофакторна автентифікація поштового облікового запису*** **Мета:** 1) пересвідчитись у відсутності або наявності витоку власних автентифікаційних даних; 2) відпрацювати навички налаштування двофакторної автентифікації для різних облікових записів для безпечного та успішного управління у сфері IT-технологій, промисловому менеджменті, управлінні культурними проєктами та стартапами креативних індустрій (у сфері IT-технологій, арт-, івент-, медіа-, сфера дозвілля, дизайн, PR-бізнес, в професійній діяльності у сфері виробництва та управління якістю і безпечністю харчових продуктів, зокрема у сфері ресторанних технологій, у сфері менеджменту тощо). **Завдання:** 1) за адресами https://haveibeenpwned.com , https://monitor.firefox.com перевірити наявність власних поштових облікових записів у «зливах», де фігурують вкрадені дані автентифікації. у випадку знаходження поштових облікових записів у «зливах» терміново змінити паролі на відповідних ресурсах та, за можливості, налаштувати двофакторну автентифікацію; 2) створити безкоштовні особисті поштові облікові записи в доменах gmail.com та protonmail.com. Налаштувати двофакторну автентифікацію через Google Authenticator для облікових записів gmail.com та protonmail.com.	2	4
Лабораторне заняття №12 ***Використання цифрових підписів у сфері IT-технологій, на основі застосування наукових і математичних принципів, для успішного***	2	4

управління культурними проєктами та стартапами креативних індустрій тощо **Мета:** зрозуміти концепції цифрового підпису**,** оскільки мета цифрового підпису полягає в тому, щоб запобігти підробці та інперсоніфікації цифрових повідомлень **Завдання:** продемонструвати використання цифрових підписів (використовувати веб-сайт для перевірки підпису документа); продемонструвати перевірку цифрового підпису; створення власного цифрового підпису.		
Лабораторне заняття №13 **Резервне копіювання даних користувача до зовнішнього сховища у сфері ІТ-технологій, безпечного та успішного управління культурними проєктами та стартапами, креативних індустрій, в професійній діяльності у сфері виробництва та управління якістю і безпечністю харчових продуктів, зокрема у сфері ресторанних технологій** **Мета:** 1) Використання локального зовнішнього диску для резервного копіювання даних; 2) Використання віддаленого диску для резервного копіювання даних. **Завдання:** Дослідити переваги резервного копіювання даних на локальний зовнішній диск. Робота фокусується на Microsoft Backup Utility для виконання резервних копій на локальні зовнішні диски. У другій частині лабораторної роботи використати службу Dropbox для резервного копіювання даних на віддалений або хмарний диск.	2	4
Лабораторне заняття №14 ***Криптографічний вид захисту інформації. Поняття шифрування файлів, папок, повідомлень. Засоби здійснення шифрування інформації.*** Мета: ознайомитися з поняттям криптографії, способами шифрування файлів, папок, повідомлень та криптографічними методами захисту інформації, розглянути основні засоби здійснення криптографічного захисту інформації; засвоїти принципи, технологію роботи шифрування та дешифрування файлів. **Завдання:** 1) Шифр Цезаря — симетричний алгоритм шифрування підстановками. Використовувався римським імператором Юлієм Цезарем для приватного листування. Принцип дії полягає в тому, щоб циклічно зсунути алфавіт, а ключ — це кількість літер, на які робиться зсув. Користуючись алфавітом АБВГҐДЕЄЖЗИІЇЙКЛМНОПРСТУФХЦЧШЩЬЮЯ та використовуючи в якості ключа власний номер в журналі (номер по порядку) зашифрувати повідомлення та записати даний шифр в звіт. «Шифр Цезаря має замало ключів — на одиницю менше, ніж літер в абетці. Тому перебрати усі ключі не складає особливої роботи. Дешифрування з одним з ключів дасть нам вірний відкритий текст». 2) Створення і шифрування повідомлення за допомогою інтерактивних методів. У сучасних мережах використовують багато алгоритмів шифрування різних типів. Одним із найбільш безпечних є симетричний алгоритм блокового шифрування (AES). Використовуватимемо засіб, який можна отримати за наступним посиланням: http://aesencryption.net/. Тому будемо використовувати цей алгоритм у роботі для шифрування та дешифрування для	2	4

успішного управління культурними проєктами та стартапами креативних індустрій.		

** всі лабораторні завдання виконуються на основі інтерактивних методів навчання у комп'ютерному середовищі*

Критерії оцінювання лабораторної роботи студента

Усний виступ та виконання письмового завдання, тестування, %	Критерії оцінювання
100%	В повному обсязі володіє навчальним матеріалом, вільно самостійно та аргументовано його викладає під час усних виступів та письмових відповідей, глибоко та всебічно розкриває зміст теоретичних питань та лабораторних завдань, використовуючи при цьому обов'язкову та додаткову літературу. Правильно вирішив усі тестові завдання.
80%	Достатньо повно володіє навчальним матеріалом, обґрунтовано його викладає під час усних виступів та письмових відповідей, в основному розкриває зміст теоретичних питань та лабораторних завдань, використовуючи при цьому обов'язкову літературу. Але при викладанні деяких питань не вистачає достатньої глибини та аргументації, допускаються при цьому окремі несуттєві неточності та незначні помилки. Правильно вирішив більшість тестових завдань
60%	В цілому володіє навчальним матеріалом викладає його основний зміст під час усних виступів та письмових відповідей, але без глибокого всебічного аналізу, обґрунтування та аргументації, без використання необхідної літератури допускаючи при цьому окремі суттєві неточності та помилки. Правильно вирішив половину тестових завдань.
40%	Не в повному обсязі володіє навчальним матеріалом. Фрагментарно, поверхово (без аргументації та обґрунтування) викладає його під час усних виступів та письмових відповідей, недостатньо розкриває зміст теоретичних питань та лабораторних завдань, допускаючи при цьому суттєві неточності, правильно вирішив меншість тестових завдань.
20%	Частково володіє навчальним матеріалом не в змозі викласти зміст більшості питань теми під час усних виступів та письмових відповідей, допускаючи при цьому суттєві помилки. Правильно вирішив окремі тестові завдання.
0%	Не володіє навчальним матеріалом та не в змозі його викласти, не розуміє змісту теоретичних питань та практичних завдань. Не вирішив жодного тестового завдання.

САМОСТІЙНА РОБОТА

Навчальна діяльність	Робочий час студента (год.)	Оцінювання (бал)
1	2	3
Тема 1. Кіберпростір і кібербезпека – головні ознаки нової інформаційної цивілізації *Самостійна робота студентів* Вивчення лекційного матеріалу. Опрацювати матеріал: «Наслідки порушення кібербезпеки», поняття «кіберзлочинець» та мотиви кіберзлочинів»; «Класифікація зловмисків та загроз» у сфері ІТ-технологій, на основі застосування наукових і математичних принципів здійснювати проектування, аналіз, верифікацію, валідизацію, запровадження та підтримку комп'ютерного програмного забезпечення, використовуючи різні мови програмування.	12	1
Тема 2. Національна система кібербезпеки України. *Самостійна робота студентів* Вивчення лекційного матеріалу; опрацювати матеріал: «Суб'єкти забезпечення інформаційної безпеки як складової національної безпеки України»; організаційна структура охорони державної таємниці.	12	1
Тема 3. Сутність та основні процедури керування кібербезпекою *Самостійна робота студентів* Вивчення лекційного матеріалу; опрацювати матеріал: проблеми захисту даних під час передачі, проблеми захисту даних у процесі обробці.	8	1
Тема 4. Кібератаки, загрози та їх властивості. Характеристика сучасних кібератак *Самостійна робота студентів* Вивчення лекційного матеріалу; опрацювати матеріал: «Кіберзагрози через Інтернет-сервіси. Поширення кіберзагроз. Кіберзагрози підвищеної складності. Проаналізувати: атака "Відмова в обслуговуванні" (DoS); розподілена DoS атака (Distributed DoS Attack, DDoS); отруєння SEO**.**	10	1
Тема 5. Дезінформація як елемент кібератак. Сценарії розвитку та методи протидії *Самостійна робота студентів* Вивчення лекційного матеріалу; опрацювати матеріал: види маніпуляцій: маніпуляції новинами; маніпуляції експертними оцінками; маніпуляції повідомленнями; маніпуляції результатами досліджень	8	1
Тема 6. Комп'ютерна вірусологія *Самостійна робота студентів* Вивчення лекційного матеріалу. Ознайомитись із інформацією про клавіатурних шпигунів (кейлогерів); класифікація комп'ютерних	10	1

1	2	3
вірусів; алгоритми роботи вірусів; типи шкідливого програмного забезпечення (ШПЗ. Опрацювати питання що стосується розповсюдження та симптомів зараження рекламним шкідливим програмним забезпеченням (adware)		
Тема 7. Соціальна інженерія *Самостійна робота студентів* Вивчення лекційного матеріалу; опрацювати матеріал: «Тактики соціальної інженерії», «Розвідка та збір інформації із відкритих джерел».	10	1
Лекція 8. Соціотехнічна безпека: проблемні аспекти *Самостійна робота студентів* Вивчення лекційного матеріалу; опрацювати матеріал: «Поняття соціотехнічної системи та її властивостей»; «Методи забезпечення інформаційної і кібербезпеки»; «Соціальні мережі: особливості, основні поняття та визначення».	10	1
Тема 9. Безпека спілкування в кіберпросторі *Самостійна робота студентів.* Вивчення лекційного матеріалу; опрацювати матеріал: «Безпечне користування мережею «Інтернет»; «Безпека браузерів»; «Безпека даних», «Безпечне користування месенджерами»; «Безпечне користування мережами WI-FI».	10	1
Тема 10. Особливості економічної діяльності суб'єктів господарювання в кіберпросторі *Самостійна робота студентів* Вивчення лекційного матеріалу; опрацювати матеріал: «Стійкий пароль. Оновлення паролів та парольних фраз». Безпека користування соціальними мережами; головні правила роботи з мобільними пристроями; безпека мобільних пристроїв; блокування доступу до пристрою; безпечна робота в мультимедійних засобах спілкування; забезпечення безпеки особистої поштової скриньки	8	1
Тема 11. Безпека цифрового простору суб'єктів господарювання *Самостійна робота студентів* Вивчення лекційного матеріалу; опрацювати матеріал: «Засоби блокування технічних каналів витоку інформації»	8	1
Тема 12. Безпека Інтернету-речей *Самостійна робота студентів.* Вивчення лекційного матеріалу; опрацювати матеріал: «Кібератаки на IoT-пристрої. Mirai. Stuxnet. Ланцюжкова реакція».	10	1
Тема 13. Системи захисту інформації на проникнення *Самостійна робота студентів* Вивчення лекційного матеріалу; опрацювати матеріал: «Історичні приклади стеганосистем. Галузі застосування стеганографії», «методи та моделі стеганографії; комп'ютерна і цифрова стеганографія»; «Технології маскування даних», Апаратні засоби, мережні технології та хмарні технології захисту..	8	2

1	2	3
Тема 14. Основні методи забезпечення кібербезпеки суб'єкта господарювання ***Самостійна робота студентів.*** Вивчення лекційного матеріалу; Ознайомитись поглиблено «Типи шифрування. Шифрування за допомогою закритого ключа. Процес симетричного шифрування. Типи криптографічних перетворень». Опрацювати теми: «Поняття криптографії та типи криптографічних перетворень»	8	1

Критерії оцінювання самостійної роботи студента

Оцінювання одного завдання у відсотковому еквіваленті	Критерії оцінювання роботи
40%	Детальний розгляд сутності та вмісту основних джерел. Подання фактів, ідей і результатів досліджень у логічній послідовності. Правильно проаналізовано поточний стан дослідження проблеми та зроблено огляд перспектив подальшого розвитку даного питання.
40%	Обґрунтованість аргументів, підтвердження особистого ставлення, пропозиції стосовно вирішення завдання, встановлення напрямків аналізу.
20%	Оформлення звіту у відповідності вимог

Сума балів, накопичених здобувачем вищої освіти за виконання всіх видів поточних навчальних завдань (робіт) на лабораторних заняттях та на підсумковому модульному контролі, свідчить про ступінь оволодіння ним програмою навчальної дисципліни на конкретному етапі її вивчення. Протягом семестру студенти можуть набрати від 0 до 100 балів, що переводяться у національну шкалу оцінювання і відповідно у шкалу ЄКТС. Кількість балів відповідає певному рівню засвоєння дисципліни:

Критерії оцінювання

За системою ДТЕУ	За шкалою ECTS	За національною системою	Визначення
90-100	A	5 (відмінно)	Повно та ґрунтовно засвоїв всі теми навчальної програми вміє вільно та самостійно викласти зміст всіх питань програми навчальної дисципліни, розуміє її значення для своєї професійної підготовки, повністю виконав усі завдання кожної теми та поточного модульного контролю в цілому. Брав участь в олімпіадах, конкурсах, конференціях.

За системою ДТЕУ	За шкалою ECTS	За національною системою	Визначення
82-89	B	4 (дуже добре)	Недостатньо повно та ґрунтовно засвоїв окремі питання робочої програми. Вміє самостійно викласти зміст основних питань програми навчальної дисципліни, виконав завдання кожної теми та модульного поточного контролю в цілому.
75-81	C	4 (добре)	Недостатньо повно та ґрунтовно засвоїв деякі теми робочої програми, не вміє самостійно викласти зміст деяких питань програми навчальної дисципліни. Окремі завдання кожної теми та модульного поточного контролю в цілому виконав не повністю.
69-74	D	3 (задовільно)	Засвоїв лише окремі теми робочої програми. Не вміє вільно самостійно викласти зміст основних питань навчальної дисципліни, окремі завдання кожної теми модульного контролю не виконав.
60-68	E	3 (достатньо)	Засвоїв лише окремі питання навчальної програми. Не вміє достатньо самостійно викласти зміст більшості питань програми навчальної дисципліни. Виконав лише окремі завдання кожної теми та модульного контролю в цілому.
35-59	Fx	2 (незадовільно)	Не засвоїв більшості тем навчальної програми не вміє викласти зміст більшості основних питань навчальної дисципліни. Не виконав більшості завдань кожної теми та модульного контролю в цілому.
1-34	F	2 (незадовільно)	Не засвоїв навчальної програми, не вміє викласти зміст кожної теми навчальної дисципліни, не виконав модульного контролю.

СПИСОК РЕКОМЕНДОВАНИХ ДЖЕРЕЛ

Основний

1. Даник Ю.Г. Основи кібербезпеки та кібероборони: підручник / Ю.Г. Даник, П.П. Воробієнко, В.М. Чернега. – [Видання друге, перероб. та доп.]. – Одеса.: ОНАЗ ім. О.С. Попова, 2019. − 320 с. ISBN 978-617-582-069-8

2. Бурячок В.Л. Інформаційна та кібербезпека: соціотехнічний аспект: підручник / [В. Л. Бурячок, В. Б. Толубко, В. О. Хорошко, С. В. Толюпа]; за заг. ред. д-ра техн. наук, професора В. Б. Толубка.− К.: ДУТ, 2015.− 288 с.

3. Безпека інформаційних систем: навч. посіб. / В. І. Пашорін, Ю. В. Костюк. – Київ: Держ. торг.-екон. ун-т, 2022. – 376 с.

4. Гребенюк А.М. Основи управління інформаційною безпекою: навч. посібник / А.М. Гребенюк, Л.В. Рибальченко. Дніпро: Дніпроп. держ. унт внутріш. справ, 2020. – 144 с.

Додатковий

5. Захист систем електронних комунікацій: навч.посіб./ В.О. Хорошко, О.В. Криворучко, М.М. Браіловський та ін. – Київ: Київ. нац. торг.-екон. ун-т, 2019. – 164 с.

6. Основи кіберпростору, кібербезпеки та кіберзахисту. Навч. посіб. / В. М. Богуш, В. В. Богуш, В. Д. Бровко, В. П. Настрадін; під. ред. В. М. Богуша. — К.: Видавництво Ліра-К, 2020. — 554 с. ISBN 978-617-7844-54-8.

7. Методичний посібник для тренерів з питань кібергігієни у рамках спеціальної професійної (сертифікатної) програми підвищення кваліфікації: Практикум. – Київ: ВАІТЕ, 2021. – 106 с.

8. Грабар І. Г. Безпекова синергетика: кібернетичний та інформаційний аспекти: монографія / І. Г. Грабар, Р. В. Грищук, К. В. Молодецька; за заг. ред. д.т.н., проф. Р. В. Грищука. – Житомир: ЖНАЕУ, 2019. – 280 с.

9. Технології інтернету речей. Навчальний посібник [Електронний ресурс]: навч. посіб. для студ. спеціальності 126 «Інформаційні системи та технології», спеціалізація «Інформаційне забезпечення робототехнічних систем» / Б. Ю. Жураковський, І.О. Зенів; КПІ ім. Ігоря Сікорського. – Електронні текстові дані (1 файл: 12,5 Мбайт). – Київ: КПІ ім. Ігоря Сікорського, 2021. – 271 с.

10. Указ Президента України від 15 березня 2016 року № 96/2016 «Про рішення Ради національної безпеки і оборони України» від 27 січня 2016 року «Про Стратегію кібербезпеки України».

11. Закон України «Про основні засади забезпечення кібербезпеки України» // Відомості Верховної Ради України, 2017. – № 45. – Ст.403.

12. Закон України «Про оборону України» // Відомості Верховної Ради України. – 2017. – № 45. – Ст.403.

13. Основи інформаційної безпеки: навч. посібник / В. Б. Вишня, О. С. Гавриш, Е. В. Рижков. Дніпро: Дніпроп. держ. ун-т внутріш. справ, 2020. 128 с.

Інтернет-ресурси

14. Cisco -Україна. URL: https://www.cisco.com

15. Annual Threat Reports. URL: https://www.fireeye.com/current-threats/annual-threat-report.html

16. European union agency for cybersecurity. URL: https://www.enisa.europa.eu.

**Курсивом зазначені джерела, що є в наявності в бібліотеці ДТЕУ*

7. Контроль та оцінювання результатів навчання:

Положення про оцінювання результатів навчання студентів і аспірантів наказ ДТЕУ №45 від 03.02.2022р. (Електронний ресурс. Точка доступу: https://knute.edu.ua/file/MjkwNQ==/66b0fa9bc55ebfa216b4efc74c200e04.pdf)

Під час вивчення дисципліни викладачем здійснюється поточний та підсумковий контроль. Поточний контроль та оцінювання передбачає:

- перевірку рівня засвоєння теоретичного матеріалу (тестування за матеріалами лекції, який здійснюється на початку кожної наступної лекції з використанням 365 Office);
- захист лабораторних робіт (проходить під час наступної лабораторної роботи);

- перевірка засвоєння матеріалу, що винесений на самостійне опрацювання під час фронтального опитування на лекції.

8. Політика навчальної дисципліни:

8.1. Відвідування лекційних та лабораторних занять: відвідування лекційних та лабораторних занять є обов'язковим. Допускаються пропуски занять з таких поважних причин, як хвороба (викладачу надається копія довідки від медичного закладу), участь в олімпіаді, творчому конкурсі тощо за попередньою домовленістю та згодою викладача за умови дозволу деканату (надаються документи чи інші матеріали, які підтверджують заявлену участь у діяльності студента).

8.2. Відпрацювання пропущених занять: відпрацювання пропущених занять є обов'язковим незалежно від причини пропущеного заняття. Лекційне заняття має бути відпрацьоване до наступної лекції на консультації викладача з використанням ПЗ 365 Office Teams. Відпрацювання лекційного матеріалу передбачає вивчення пропущеного теоретичного матеріалу та складання тесту за цим матеріалом. Лабораторне заняття відпрацьовується під час консультації викладача (розклад консультацій на сайті).

8.3. Правила поведінки під час занять: обов'язковим є дотримання техніки безпеки в комп'ютерних лабораторіях. Студенти повинні приймати активну участь в обговоренні навчально матеріалу ознайомившись з ним напередодні (навчальний матеріал надається викладачем). Мобільні пристрої дозволяється використовувати лише під час он-лайн тестування та підготовки практичних завдань в процесі заняття. Задля зручності, дозволяється використання ноутбуків та інших електронних пристроїв під час навчання в комп'ютерних аудиторіях (за взаємною згодою всіх учасників освітнього процесу)

8.4. За порушення академічної доброчесності студенти будуть притягнені до академічної відповідальності у відповідності до положення про дотримання академічної доброчесності педагогічними, науково-педагогічними, науковими працівниками та здобувачами вищої освіти ДТЕУ (Наказ ДТЕУ від 03.02.2022 №45. (Електронний ресурс. Точка доступу: https://knute.edu.ua/file/MjkwMjQ=/271e66c30b3162b933b9bf8caa4c101c.pdf)