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

БЕЗПЕКА ІНФОРМАЦІЙНИХ СИСТЕМ ТА МЕРЕЖ / SECURITY OF INFORMATION SYSTEMS AND NETWORKS
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: Тищенко Дмитро Олександрович,

вчене звання та посада: кандидат економічних наук, доцент кафедри інженерії програмного забезпечення та кібербезпеки;

контактний телефон: (044)- 513-98-62;

e-mail: tyshchenko_d@knute.edu.ua

наукові інтереси: кібербезпека, електронний документообіг, інтернет-технології в бізнесі, web-дизайн, інформаційні технології та системи

1. **Дисципліна: «БЕЗПЕКА ІНФОРМАЦІЙНИХ СИСТЕМ ТА МЕРЕЖ»,**

- рік навчання: II-IV;
- семестр навчання: 3-8;
- 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: 504, 510, 510а, 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 «Інформаційні системи і технології в

професійній діяльності», «Іноземна мова за професійним спрямуванням», «Об'єктно-орієнтоване програмування», «Архітектура комп'ютера».

- **постреквізити:** дисципліна надає студентам необхідні знання та навички, які будуть корисні при вивченні дисциплін «Людино-машинна взаємодія», «Штучний інтелект», «Методи і засоби передачіданих» при проходженні практичної підготовки, підготовки та захисту кваліфікаційної роботи, у подальшій професійній діяльності.

Програмні результатів навчання:

ПР04	знати і застосовувати професійні стандарти і інші нормативно-правові документи в галузі інженерії програмного забезпечення.
ПР16	мати навички командної розробки, погодження, оформлення і випуску всіх видів програмної документації.
ПР20	знати підходи щодо оцінки та забезпечення якості програмного забезпечення
ПР22	знати та вміти застосовувати методи та засоби управління проектами.
ПР24	вміти проводити розрахунок економічної ефективності програмних систем.

4. Характеристика дисципліни:

4.1. <u>Призначення навчальної дисципліни:</u> Дисципліна «Безпека інформаційних систем та мереж» є важливою складовою підготовки сучасних фахівців з розробки інформаційних технологій. Завданням дисципліни є ознайомлення студентів із законодавчим, організаційним, інженерно-технічним і програмними рівнями безпеки інформаційних систем, засобами і методами управління контролем доступу в комп'ютерних системах, методами ідентифікації і аутентифікації користувачів і ресурсів інформаційних систем, особливостями захисту інформації в локальних і корпоративних мережах, навчити їх реалізовувати практично правила політики безпеки.

4.2. <u>Метою вивчення дисципліни:</u> метою вивчення дисципліни «Безпека інформаційних систем та мереж» є формування теоретичних знань та практичних навичок, необхідних для ефективного використання інформаційних технологій в інформаційних системах і мережах а також запобігання розголошенню, витоку і неправомірному оволодінню інформацією, протиправним діям щодо знищення, модифікації, копіювання і блокування інформації.

4.3. <u>Задачі вивчення дисципліни:</u> Основними завданнями вивчення дисципліни " Безпека інформаційних систем та мереж " є формування у студентів компетентностей, що набуває здобувач вищої освіти по закінченню вивчення даної дисципліни:

Загальні компетентності:

К01	Здатність до абстрактного мислення, аналізу та синтезу.
К02	Здатність застосовувати знання у практичних ситуаціях.
К03	Здатність спілкуватися державною мовою як усно, так і письмово.
К06	Здатність до пошуку, оброблення та аналізу інформації з різних джерел.

Спеціальні (фахові, предметні) компетентності:

К17	Здатність формулювати та забезпечувати вимоги щодо якості програмного забезпечення у відповідності з вимогами замовника, технічним завданням та стандартами.
К18	Здатність дотримуватися специфікацій, стандартів, правил і рекомендацій в професійній галузі при реалізації процесів життєвого циклу.

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. Безпека інформаційних систем в умовах функціонування глобальних мереж. *План лекції:* 1. Актуальність, цілі і завдання інформаційної безпеки. 2. Принципи, головні задачі та функції безпеки інформаційних систем. 3. Види можливих порушень в роботі інформаційної системи. 4. Основні поняття і класифікація загроз. Основні загрози доступності,цілісності та конфіденційності інформації. 5. Модель інформаційної безпеки організації: структура і компоненти.Засоби безпеки інформаційних систем і мереж. **Список рекомендованих джерел:** *Основний*: 2, 3, 4. *Додатковий*: 10, 11. *Інтернет-джерела*: 15.	**4**
Лекція №2. Законодавство по захисту інформації в інформаційних системах *План лекції:* 1 Правові норми забезпечення безпеки і захисту інформації. 2. Українське законодавство в галузі інформаційної безпеки. 3. Зарубіжне законодавство в галузі інформаційної безпеки. **Список рекомендованих джерел:** *Основний: 1, 2.*	**2**

1	2
Додатковий: 6, 7. *Інтернет-джерела: 15-16.*	
Лекція №3. Організаційний захист інформації в інформаційних системах *План лекції* 1. Поняття та принципи політики інформаційної безпеки. 2. Впровадження програми безпеки на об'єктах інформаційної діяльності. 3. Організаційна структура системи забезпечення безпеки інформації. 4. Міжнародні та вітчизняні стандарти в галузі управління, оцінки та аудиту інформаційної безпеки. **Список рекомендованих джерел:** *Основний: 2, 3, 4.* *Додатковий: 9.* *Інтернет-джерела: 15, 19*	**2**
Лекція №4. Канали витоку інформації. *План лекції*: 1. Класифікація та характеристики технічних каналів витоку інформації. 2. Радіоканали витоку інформації та їх класифікація. 3. Класифікація та характеристики візуально-оптичних каналів витокуінформації. 4. Електричні канали витоку інформації. **Список рекомендованих джерел:** *Основний: 2, 3, 4.* *Додатковий: 9, 12.* *Інтернет-джерела: 15-16.*	**2**
Лекція №5. Технічний захист інформації і об’єкти захисту *План лекції:* 1. Властивості об’єктів захисту в інформаційній системі 2. Активні та пасивні методи забезпечення технічного захисту вінформаційних системах 3. Захист інформації від витоку по технічним каналам. Апаратні засоби захисту. 4. Програмні засоби захисту інформації в інформаційних системах**.** **Список рекомендованих джерел:** *Основний: 1, 2.* *Додатковий: 11.* *Інтернет-джерела: 15.*	**2**
Лекція №6. Технічний захист інформації і об’єкти захисту *План лекції:* 1. Ідентифікація, автентифікація та авторизація суб'єктів інформаційноїсистеми. 2. Сутність методів ідентифікації таавтентифікації. 3. Біометрична автентифікація **Список рекомендованих джерел:** *Основний: 1, 2.* *Додатковий: 11.* *Інтернет-джерела: 15.*	**2**

1	2
Лекція №7 Принципи криптографії. Криптографічні системи. *План лекції:* 1. Основні терміни та поняття криптографії. 2. Історія та законодавча база криптографії. 3. Перші методи шифрування перестановки та заміни застосунка. Керуваннязагрозами для застосунків. 4. Симетричні криптосистеми. Стандарт шифрування даних DES. 5. Асиметричні криптосистеми. Стандарт шифрування даних RSA. 6. Основні типи алгоритмів шифрування**.** **Список рекомендованих джерел:** *Основний: 2,3,4.* *Додатковий: 8, 9, 12, 13.* *Інтернет-джерела: 15, 17, 18, 19.*	**2**
Лекція №8 Електронний цифровий підпис *План лекції:* 1. Підпис і його властивості 2. Особливості шифрування ЕЦП 3. Склад цифрового підпису 4. Технологія застосування ЕЦП 5. Організаційне забезпечення електронного цифрового підпису. 6. Управління ключами та сертифікація ключів. **Список рекомендованих джерел:** *Основний: 2,3,4.* *Додатковий: 9, 12, 13.* *Інтернет-джерела: 16-19.*	**2**
Лекція № 9 Шкідливе програмне забезпечення *План лекції:* 1. Поняття і класифікація комп'ютерних вірусів. 2. Програми – закладки і методи захисту від них. 3. Троянські програми. 4. Черв'яки і інші шкідливі програми. 5. Антивірусні програми і комплекси. **Список рекомендованих джерел:** *Основний: 2,3,4.* *Додатковий: 9, 12, 13.* *Інтернет-джерела: 15-19.*	**2**
Лекція № 10 Шкідливе програмне забезпечення. Віртуальні захищені мережі VPN *План лекції:* 1. Аналіз загроз мережевої безпеки. 2. Види, функції та особливості роботи міжмережевих екранів. 3. Конфігурування міжмережевих екранів. 4. Класифікація та варіанти архітектури мереж VPN 5. Засоби захисту мереж VPN. **Список рекомендованих джерел:** *Основний: 2,3,4,5.* *Додатковий: 9, 12, 14.*	**2**

1	2
Інтернет-джерела: 15, 16, 19	
Лекція № 11 Захист Wi-Fi мереж. *План лекції:* 1. Безпека безпроводових мереж. 2. Погрози і ризики безпеки безпроводових мереж. 3. Протоколи безпеки безпроводових мереж. **Список рекомендованих джерел:** *Основний: 2,3,4,5.* *Додатковий: 9, 12, 14.* *Інтернет-джерела: 15, 17-19.*	**2**

ЛАБОРАТОРНІ ЗАНЯТТЯ

Навчальна діяльність	Робочий час студента (год.)	Оцінювання (бал)
1	2	3
ТЕМА 3. АДМІНІСТРАТИВНЕ ТА ОРГАНІЗАЦІЙНЕ ЗАБЕЗПЕЧЕННЯ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ **Список рекомендованих джерел**: *Основний: 2, 3, 4.* *Додатковий: 9.* *Інтернет-джерела: 15, 19* **Лабораторна робота №1. Створення політики інформаційної безпеки дляорганізації** **Мета:** вміти побудувати план захисту інформації в інформаційній системі **Завдання:** 1. Проаналізувати та систематизувати існуючи методики розробки політик безпеки на підприємстві (за варіантом). 2. Створити документ с викладенням політики інформаційної безпеки (за варіантом). 3. Підготувати звіт-презентацію по розробці, розгортанню та ефективномувикористанню політики інформаційної безпеки. 4. Скласти план захисту інформації в інформаційній системі. **Результати навчання** • Опанування адміністративнихметодів захисту інформаційних системі мереж; • розуміти особливості організаційних заходів щодо захисту інформації в інформаційних системах. • вміти розробляти основні положення політикибезпеки і програму їїреалізації	**4**	**10**
ТЕМА 4. ПРОГРАМНО–ТЕХНІЧНЕ ЗАБЕЗПЕЧЕННЯ		

1	2	3
ІНФОРМАЦІЙНОЇ БЕЗПЕКИ Список рекомендованих джерел: *Основний: 2, 3, 4.* *Додатковий: 9, 12.* *Інтернет-джерела: 15-16.* **Лабораторна робота №2. Засоби несанкціонованого доступу доінформації** **Мета:** знати засоби несанкціонованого доступу до інформації. **Завдання:** 1. Проаналізувати та систематизувати існуючі засоби несанкціонованого доступу до інформації (за варіантом): – по акустичних каналах; – через лінії електроживлення та заземлення; – через лінії зв'язку; – через візуально-оптичні канали; – через побічні електромагнітні випромінювання та наводки. 2. Підготувати звіт-презентацію по розглянутих засобах несанкціонованогодоступу до інформації. **Результати навчання** • Мати уявлення реєстрацію порушення режиму безпеки • Розуміти, як створювати захист інформації за допомогою технічнихзасобів; • вміти захищати інформаційні системиза допомогою програмних засобів та створювати захист інформації за допомогою програмних засобів;	**4**	**10**
Лабораторна робота №3. Методи і засоби технічного захисту інформації **Мета:** зрозуміти особливості методів і засобів технічного захисту інформації. **Завдання:** 1. Проаналізувати та систематизувати існуючи засоби захисту інформаціївід витоку (за варіантом): o по акустичних каналах ; o через лінії електроживленя тазаземлення; o через лінії зв'язку; o -через візуально-оптичні канали; o через побічні електромагнітні випромінювання та наводки. o через засоби телевізійної охорони. 2. Підготувати звіт-презентацію по розглянутих технічних засобах захистуінформації. **Результати навчання** • навчитись використовувати системні ресурси для	**4**	**10**

1	2	3
захисту інформації та захищати інформаційні системиза допомогою програмних засобів; • знати як використовувати системні ресурси длязахисту інформації.		
Лабораторна робота №4. Парольний захист. Безпека зберігання даних вОС Microsoft Windows **Мета:** Вияснення паролю користувача з використанням утіліти для зламу пароля. Знати і розуміти концепцію безпека зберігання даних в ОС MicrosoftWindows. **Завдання:** 1. Проаналізувати та систематизувати існуючи засоби парольного захистуархівних файлів із паролями різної довжини й структури. 2. Проаналізувати захищеність даних паролями 3. Підготувати звіт за результатами виконання лабораторної роботи. 4. Створити тіньові копії спільних каталогів. 5. Виконати повну й додаткову архівацію за допомогою програми Backup. 6. Виконати відновлення даних за допомогою програми Backup. 7. Створити дзеркальні тома в ОС Windows Server **8.** Підготувати звіт про виконання лабораторної роботи **Результати навчання** ○ навчитись використовувати системні ресурси для захисту інформації та захищати інформаційні системи за допомогою програмних засобів	**4**	**10**
Лабораторна робота №5. Дослідження та захист реєстру операційної системи Windows *Мета*:Концепція дослідження та захист операційної системи Windows. **Завдання:** 1. Підготувати віртуальну машину з ОС Windows для виконання лабораторної роботи. 2. Підготувати текстовий файл, у який внести задані за варіантом настроювання реєстру. 3. Запустити файл настроювання реєстру й перевірити роботу внесених змін. 4. Скласти звіт по роботі **Результати навчання** Дослідити захист операційної системи та навчитись перевіряти внесення змін у роботу системи.	**2**	**5**
ТЕМА 5. ОСНОВИ КРИПТОГРАФІЧНОГО ЗАХИСТУ ІНФОРМАЦІЇ **Список рекомендованих джерел:** *Основний: 2,3,4.*		

1	2	3
Додатковий: 8, 9, 12, 13. *Інтернет-джерела: 15, 17, 18, 19.* **Лабораторна робота № 6. Створення алгоритму криптографічногозахисту** *Мета*: Ознайомлення з порядком побудови алгоритму криптографічного захисту. **Завдання:** 1. Ознайомитися з методом шифрування за варіантом. 2. Розробити блок-схему алгоритму шифрування та розшифровування. 3. Реалізувати формальні моделі у вигляді двох підсистем модуля змінімальним інтерфейсом. 4. Описати особливості реалізації завдання та варіанти застосуваннярозробленого модуля. **Результати навчання** ○ Вивчити основні поняття криптографічного і стеганографічного захисту інформації ○ Навчитись застосовувати засоби кібербезпеки	**2**	**5**
ТЕМА 7. БЕЗПЕЧНА РОБОТА В КОМП'ЮТЕРНИХ МЕРЕЖАХ **Список рекомендованих джерел:** *Основний: 2, 3, 4, 5* *Додатковий: 9, 12, 14* *Інтернет-джерела: 15, 16, 19* **Лабораторна робота № 7. Дослідження системи захищеногоелектронного листування PGP** **Мета:** дослідити систему захищеного електронного листування PGP **Завдання:** 1. Створити ключі в програмі PGP. 2. Зашифрувати та надати електронний цифровий підпис електронномуповідомленню 3. Налаштувати систему захищеного електронного листування. 4. Підготувати звіт про виконання лабораторної роботи **Результати навчання** - Вміти організовувати безпечну роботу в комп'ютерних мережах та використовувати електронну пошту длязахищеного обміну інформацією	**4**	**10**

** 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. ОСНОВНІ ПОЛОЖЕННЯ ТЕОРІЇ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ **Список рекомендованих джерел**: *Основний*: 2, 3, 4.		

1	2	3
Додатковий: 10, 11. *Інтернет-джерела*: 15. **Питання винесені на самостійне опрацювання:** 1. Розголошування та витік інформації. 2. Несанкціонований доступ до системи або мережі 3. Порушники інформаційної безпеки. 4. Класифікація порушників. 5. Методика вторгнення до інформаційної системи	**20**	**10**
ТЕМА 2. ПРАВОВЕ ЗАБЕЗПЕЧЕННЯ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ **Список рекомендованих джерел:** *Основний: 1, 2.* *Додатковий: 6, 7.* *Інтернет-джерела: 15-16* **Питання винесені на самостійне опрацювання:** 1. Правові норми забезпечення безпеки і захисту інформації. 2. Міжнародні стандарти інформаційної безпеки.	**20**	**5**
ТЕМА 3. АДМІНІСТРАТИВНЕ ТА ОРГАНІЗАЦІЙНЕ ЗАБЕЗПЕЧЕННЯ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ **. Список рекомендованих джерел:** *Основний: 2, 3, 4.* *Додатковий: 9.* *Інтернет-джерела: 15, 19.* **Питання винесені на самостійне опрацювання:** 1. Критерії оцінювання захищеності інформаційної системи. "Критерії оцінки довірених комп'ютерних систем" ("Помаранчева книга"). 2. Міжнародний стандарт побудови ефективної системи безпеки ISO 17799. 3. Базова і спеціалізовані політики безпеки.	**20**	**5**
ТЕМА 4. ПРОГРАМНО–ТЕХНІЧНЕ ЗАБЕЗПЕЧЕННЯ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ **Список рекомендованих джерел:** *Основний: 2, 3, 4.* *Додатковий: 9, 12.* *Інтернет-джерела: 15-16.* **Питання винесені на самостійне опрацювання:** 1. Класифікація та характеристики матеріально-речових каналіввитоку інформації. 2. Радіозакладні пристрої та їх класифікація 3. Технічні засоби перехоплення інформації.	**20**	**5**

1	2	3
4. Методи та види несанкціонованого доступу до інформаційних систем. 5. Системи технічної та фізичної охорони об'єктів інформаційної діяльності. 6. Основні етапи створення комплексу технічного захисту на об'єктіінформаційної діяльності 7. Технічні засоби пасивного виявлення радіозакладних пристроїв: - індикатори електромагнітних випромінювань, інтерцептори,радіочастотоміри та скануючи приймачі. 8. Перспективні системи технічного захисту інформації		
ТЕМА 5. ОСНОВИ КРИПТОГРАФІЧНОГО ЗАХИСТУ ІНФОРМАЦІЇ **Список рекомендованих джерел:** *Основний: 2,3,4.* *Додатковий: 8, 9, 12, 13.* *Інтернет-джерела: 15, 17, 18, 19* **Питання винесені на самостійне опрацювання:** 1. Одноалфавітні системи шифрування 2. Багатоалфавітні системи шифрування 3. Захист документів Microsoft Office від несанкціонованого доступу 4. Шифруюча файлова система	**20**	**5**
ТЕМА 6. ЗАХИСТ ВІД РУЙНУЮЧИХ ПРОГРАМНИХ ДІЙ **Список рекомендованих джерел:** *Основний: 2,3,4.* *Додатковий: 9, 12, 13.* *Інтернет-джерела: 15-19.* **Питання винесені на самостійне опрацювання:** 1.Правила використання стороннього програмного забезпечення. 2. Спам і засоби боротьби з ним..	**17**	**5**
ТЕМА 7. БЕЗПЕЧНА РОБОТА В КОМП'ЮТЕРНИХ МЕРЕЖАХ **Список рекомендованих джерел:** *Основний: 2, 3, 4,5* *Додатковий: 9,12,14* *Інтернет-ресурси 15,16, 19* **Питання винесені на самостійне опрацювання:** 1. . Правила безпечної роботи в мережах. 2. Захист на мережевому рівні. 3. Схеми мережевого захисту на базі міжмережевих екранів.	**15**	**5**

1	2	3
4. Правила користування електронною поштою. 5. Адміністрування електронної пошти. 6. Використання електронної пошти для конфіденційного обмінуінформацією		

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. Положення про технічний захист інформації в Україні від 27 вересня 1999 року № 1229/99.
2. Остапов С.Е., Євсеєв С.П., Король О.Г., Технології захисту інформації – Чернівці.- Видавничий дом «Родовід», 2018. – 471с.
3. *Пашорін В.І., Костюк Ю.В. Безпека інформаційних систем : навч. посіб. / В. І. Пашорін, Ю. В. Костюк. Київ : Держ. торг.-екон. ун-т, 2022. – 376 с.*
4. Основи управління інформаційною безпекою: навч. посібник /А.М. Гребенюк, Л.В. Рибальченко. Дніпро: Дніпроп. держ. ун- т внутріш. справ,

2020. – 144 с.
5. Єсін В. І. Безпека інформаційних систем і технологій : навчальний посібник /В. І. Єсін, О. О. Кузнецов, Л. С. Сорока. – Х. : ХНУ імені В. Н. Каразіна, 2017. – 632с.

Додатковий

6. Концепція (основи державної політики) національної безпеки України від 21 грудня 2000 року №2171-111.
7. Інструкція про порядок обліку і зберігання і використання документів, справ, видань та інших матеріальних носіїв інформації, які містять конфіденційну інформацію, що є власністю держави від 27 листопада 1998 року № 1893.
8. Положення про порядок здійснення криптографічного захисту інформації в Україні від 22 травня 1998 року № 505/98.
9. Гаврильців М.Т. Інформаційна безпека держави в системі національної безпеки України. Юридичний науковий журнал. 2020. № 2. С. 200-203.
10. Захаренко К. В. Інституційний вимір інформаційної безпеки України: трансформаційні виклики, глобальні контексти, стратегічні орієнтири. / К. В. Захаренко. Київ, 2021, 423с.
11. *Пашкова А. Т. Інформаційна безпека як складова національної безпеки А. Т. Пашкова // Безпека життєдіяльності. – Київ, 2014. – № 11. – С. 34-36.*
12. *Полянська В. Кібернетична безпека України в умовах розвитку глобальної інформаційної системи / В. Полянська // Підприємництво, господарство і право. – Київ, 2013. – № 7 (211). – С. 48-50.*
13. Турчак А.В. Основні засади державної політики забезпечення інформаційної безпеки в Україні. Інвестиції: практика та досвід. 2019. № 11. С. 123-127.
14. Інформаційна безпека. Підручник / В. В. Остроухов, М. М. Присяжнюк, О. І. Фармагей, М. М. Чеховська та ін.; під ред. В. В. Остроухова – К.: Видавництво Ліра-К, 2021. – 412 с.

Інтернет-джерела

15. Захист інформації – режим доступу: *http://www.warning.dp.ua/tel28.htm*
16. Безпека на прикладному рівні – режим доступу: *http://www.dut.edu.ua*
17. IEEE computer society. SWEBOK режим доступу: *http://www.computer.org/portal/web/swebok/htmlformat*
18. Process Models in Software Engineering – режим доступу:*http://www.ics.uci.edu/~wscacchi/Papers/SE-Encyc/Process-Models-SE- Encyc.pdf*
19. Technical writing for software engineers режим доступу: *http://www.dtic.mil/dtic/tr/fulltext/u2/a223872.pdf*

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)