КИЇВСЬКИЙ НАЦІОНАЛЬНИЙ 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 програмної інженерії та кібербезпеки

СИЛАБУС
МЕТОДИ І ЗАСОБИ ЗАХИСТУ ІНФОМАЦІЇ В КОМП'ЮТЕРНИХ СИСТЕМАХ/
METHODS AND MEANS OF PROTECTION OF INFOMATION IN COMPUTER SYSTEMS
SYLLABUS

освітній ступінь	**магістр /** master
галузь знань	**12 Інформаційні технології /** Information Technology
спеціальність	**121 Інженерія програмного забезпечення /** Software Engineering
спеціалізація	**Інженерія програмного забезпечення /** Software Engineering

Гарант освітньо-професійної програми "Інженерія програмного забезпечення" другого (магістерського) рівня вищої освіти

Завідувач кафедри програмної інженерії та кібербезпеки, д.т.н., проф. Криворучко О.В.

Київ 2019

Автори: В.І. Пашорін, канд.техн.наук, проф.

Силабус розглянуто і затверджено на засіданні кафедри програмної інженерії та кібербезпеки 10 вересня 2019 р., протокол № 3.

СИЛАБУС

МЕТОДИ І ЗАСОБИ ЗАХИСТУ ІНФОМАЦІЇ В КОМП'ЮТЕРНИХ СИСТЕМАХ/
METHODS AND MEANS OF PROTECTION OF INFOMATION IN COMPUTER SYSTEMS

SYLLABUS

освітній ступінь	**магістр /** master
галузь знань	**12 Інформаційні технології /** Information Technology
спеціальність	**121 Інженерія програмного забезпечення /** Software Engineering
спеціалізація	**Інженерія програмного забезпечення /** Software Engineering

АНОТАЦІЯ КУРСУ

1. **Викладачі**:
   1.1. **Лектор**: Пашорін Валерій Іванович,
   - к.т.н., професор кафедри програмної інженерії та кібербезпеки;
   - *педагогічний стаж* – 35 років;
   - *контактний телефон:* +38(098)244-09-47;
   - *e-mail:* vpashorin@knute.edu.ua
   - *наукові інтереси*: кібербезпека;
   - *стажування та підвищення кваліфікації*:
   - *додаткова інформація*:

   1.2. **Ассистент лектора:**
2. **Дисципліна**: «Безпека інтернет-ресурсів»,
   - рік навчання:I
   - семестр навчання: I
   - кількість кредитів: 6
   - кількість годин за семестр: 180
     - лекційних: 28
     - лабораторних: 28
     - на самостійне опрацювання: 124
   - кількість аудиторних годин на тиждень:
     - лекційних: 2
     - лабораторних: 2
3. **Час та місце проведення:**
   - аудиторні заняття - відповідно до розкладу КНТЕУ з врахуванням специфіки дисципліни передбачено аудиторіях: 504, 514;
   - поза аудиторна робота - самостійна робота студента, результат виконання якої висвітлено засобами Office 365;
4. **Пререквізити та постреквізити навчальної дисципліни:**
   - **пререквізити:** «Безпека інформаційних систем і мереж», «Операційні системи», «Архітектура комп'ютера».
   - **постреквізити:** (дициплiни та компетентності, які необхідні в трудовій діяльності фахівця)
5. **Характеристика дисципліни:**

5.1. Призначення навчальної дисципліни: Основу дисципліни «Методи і засоби захисту інформації» становить вивчення основних положень та принципів побудови та використання програмних та програмно-апаратних засобів для захисту інформації в комп'ютерних системах. Володіння сучасними технологіями роботи та методами її практичного використання в професійній діяльності стало необхідним елементом підготовки кваліфікованого інженера з інфокомунікацій. Дана дисципліна формує інженерний світогляд фахівця в галузі ІТ.

5.2. **Мета вивчення дисципліни:** формування теоретичних знань та практичних навичок необхідних для ефективного захисту інформації в комп'ютерних системах.

5.3. **Задачі вивчення дисципліни:** полягають у тому, щоб ознайомити студентів із організаційним і програмними рівнями безпеки комп'ютерних систем, засобами і методами управління контролем доступу в комп'ютерних системах, методами автентифікації користувачів і ресурсів навчити їх створювати програми безпеки на підприємстві і реалізовувати практично правила політики безпеки.

5.4. **Зміст навчальної дисципліни:** відповідає навчальній та робочій програмі, визначеній науковими досягненнями як наукові досягнення вітчизняних та закордонних вчених, а також запитам стейкхолдерів.

5.5. **План вивчення дисципліни**

Результати навчання	Навчальна діяльність	Робочий час студента (год.)	Оцінювання (бал)
1	2	3	4
Знати: основні концептуальні положення системи захисту комп'ютерних систем; класифікацію загроз інформації та міри протидії;	**Тема 1.** Захист інформації засобами операційних систем **Лекція 1. План лекції** 1. Віртуалізація як засіб забезпечення безпеки інформації в комп'ютерних системах 2. Загрози безпеці операційним системам. Поняття захищеної операційної системи 3. Основні функції підсистеми захисту операційної системи 4. Командний інтерпретатор і командні файли **Список рекомендованих джерел** Основний: 2, 3, 4 Додатковий: 10, 11	2	
Вміти: визначати порушення в роботі комп'ютерних систем	**Самостійна робота студентів** Вивчення та доповнення матеріалу лекції з питань: 1. Проблеми забезпечення безпеки операційної системи 2. Командний інтерпретатор і командні файли	4	2
Знати: засоби керування безпекою в операційних системах	**Лекція 2. План лекції** 1. Архітектура підсистеми захисту операційної системи 2. Автентифікація і авторизація суб'єктів доступу на рівні ОС	2	

1	2	3	4
	3. Розмежування доступу до об'єктів операційної системи Windows 4. Керування системними сервісами **Список рекомендованих джерел** Основний: 2, 3, 4 Додатковий: 10, 11		
* курсивом виділені інтерактивні методи навчання			
Вміти: Вибирати засоби безпеки комп'ютерних систем	**Самостійна робота студентів** Вивчення та доповнення матеріалу лекції з питань: 1. Засоби захисту в ОС Windows Підготовка до лабораторної роботи з установки віртуальної машини.	12	4
Знати: методи захисту інформації в комп'ютерних системах засобами операційних систем	**Лекція 3. План лекції** 1. Системний реєстр Windows 2. Використання системного реєстру для захисту комп'ютерних систем 3. Консоль управління MMC 4. Адміністрування та шаблони безпеки **Список рекомендованих джерел:** Основний: 2, 3, 4 Додатковий: 9, 12	2	
Вміти: Вибирати засоби безпеки	**Самостійна робота студентів** Вивчення та доповнення матеріалу лекції з питань: 1. Аудит подій безпеки в захищених версіях операційної системи	8	2
Знати: методи захисту інформації в комп'ютерних системах засобами операційних систем	**Лекція 4. План лекції** 1. Редактор групової політики 2. Аудит подій безпеки в операційній системі Windows 3. Парольний захист в Windows: формування, зберігання і використання паролів 4. Засоби захисту в UNIX-подібних операційних системах 5. Система обробки конфіденційної інформації Trusted Solaris **Список рекомендованих джерел:** Основний: 2, 3, 4 Додатковий: 9, 12	2	
Вміти: використовувати системні	**Самостійна робота студентів** Вивчення та доповнення матеріалу лекції з питань:	8	4

1	2	3	4
ресурси для захисту інформації;	1. Шаблони безпеки. Групова та локальна політики безпеки в операційній системі *Windows*		
Вміти: виконувати аудит парольного захисту; реєструвати порушення режиму безпеки і складати звіти; створювати захист інформації за допомогою програмних засобів;	**Лабораторна робота № 1** *Парольний захист та аудит парольного захисту* Завдання на лабораторну роботу: 1. Встановити та підготувати віртуальну машину з ОС Windows для виконання лабораторної роботи 2. Проаналізувати та систематизувати існуючи засоби парольного захисту архівних файлів і аккаунтів користувачів із паролями різної довжини й структури 3. Створити на робочій станції кілька локальних користувачів із паролями різної довжини й складності. 4. Проаналізувати захищеність паролями різної складності за допомогою програм аудиту парольного захисту 5. Запустити програму перехоплення й розшифровки парольних хешей. 6. Здійснити перебір паролів (методом, залежно від варіанта). 7. Протестувати пароль, за допомогою команди Test Password. 8. Підготувати звіт за результатами виконання лабораторної роботи	4	8
Вміти: використовувати системні ресурси для захисту інформації; створювати захист інформації за допомогою програмних засобів;	**Лабораторна робота № 2** *Засоби керування безпекою в операційних системах* **Завдання на лабораторну роботу:** 1. Підготувати віртуальну машину з ОС Windows Server для виконання лабораторної роботи. 2. Створити тіньові копії спільних каталогів. 3. Проаналізувати та систематизувати існуючи засоби архівації й резервного копіювання даних. 4. Виконати порівняльний аналіз даних, одержаних за допомогою різних програм архівації. 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	4	8

1	2	3	4
	8. Настроїти розмежування прав доступу користувачів і груп, за допомогою настроювання локальної політики безпеки 9. Підготувати звіт про виконання лабораторної роботи		
Вміти: виконувати налаштування групової та локальної політики безпеки в операційній системі Windows; використовувати системні ресурси для захисту інформації; розробляти індивідуальні системи управління доступом і захистом комп'ютерних систем.	**Лабораторна робота №3** *Засоби керування безпекою в операційних системах. Групова політика безпеки* **Завдання на лабораторну роботу:** 1. Підготувати віртуальну машину з ОС (за заданим варіантом) для виконання лабораторної роботи 2. Налаштувати необхідні служби ОС, що відповідають за захист інформації на локальному комп'ютері 3. Налаштувати доступ користувачів і груп до файлів і директорій операційної системи Windows 4. Налаштувати розмежування прав доступу користувачів і груп, за допомогою локальної політики безпеки 5. Проаналізувати можливості керування безпекою через шаблони безпеки в ОС Windows 6. Ознайомитися з налаштуванням групової політики безпеки та виконати зміни налаштувань за заданим варіантом 7. Настроїти захист даних локальної робочої станції за допомогою реєстру 8. Налаштувати засоби автоматичного відновлення ОС Windows 9. Підготувати звіт про виконання лабораторної роботи	4	8
	Тема 2. Криптографічні засоби захисту інформації в комп'ютерних системах **Лекція 5. План лекції** 1. Основні терміни та поняття криптографії 2. Криптографія в економічних галузях	2	
Знати: класифікацію і напрямки використання криптоалгоритмів сучасних криптосистем	3. Сучасні криптосистеми та їхні особливості **Список рекомендованих джерел:** Основний: 2-7 Додатковий: 10		
Вміти:	**Самостійна робота студентів**	12	4

1	2	3	4
створювати захист інформації за допомогою програмних засобів; використовувати системні ресурси для захисту інформації	Вивчення та доповнення матеріалу лекції, підготовка до лабораторного заняття з питань: 1. Шифри заміни і перестановки 2. Одноразові блокноти 3. Комп'ютерні алгоритми шифрування		
Знати: класифікацію і напрямки використання криптоалгоритмів сучасних криптосистем	**Лекція 6. План лекції** 1. Симетричні криптоалгоритми 2. Блокові і потокові шифри 3. Архітектура блокових шифрів 4. Мережа Фейштеля. **Список рекомендованих джерел:** Основний: 2-7 Додатковий: 8,9,10	2	
Вміти: створювати захист інформації за допомогою програмних засобів; використовувати системні ресурси для захисту інформації	**Самостійна робота студентів** Вивчення та доповнення матеріалу лекції, підготовка до лабораторного заняття з питань: 1. AES: стандарт блочних шифрів США. Шифри - фіналісти AES: шифр MARS, шифр RC6, шифр Serpent, шифр TwoFish. шифр Rijndael 2. Режими виконання алгоритмів симетричного шифрування	12	4
Знати: класифікацію і напрямки використання криптоалгоритмів сучасних криптосистем	**Лекція 7. План лекції** 1. Асиметричні криптоалгоритми 2. Стандарт шифрування даних RSA 3. Асиметричні криптосистеми на базі еліптичних кривих **Список рекомендованих джерел:** Основний: 1,2,3 Додатковий: 10	2	
Вміти: створювати захист інформації за допомогою	**Самостійна робота студентів** Вивчення та доповнення матеріалу лекції, підготовка до лабораторного заняття з питань: 1. Алгоритм Ель-Гамаля	12	4

1	2	3	4
програмних засобів; використовувати системні ресурси для захисту інформації	2. ДСТУ 7624:2014 - український національний стандарт криптографічного захисту інформації (блоковий шифр «Калина»)		
Знати: класифікацію і напрямки використання криптоалгоритмів сучасних криптосистем;	**Лекція 8. План лекції** 1. Хеш-функції і алгоритми хешування 2. Алгоритми сімейства MD та сімейства SHA **Список рекомендованих джерел:** Основний: 1,2,3 Додатковий: 9	2	
Вміти: створювати захист інформації за допомогою програмних засобів; використовувати системні ресурси для захисту інформації	**Самостійна робота студентів** Вивчення та доповнення матеріалу лекції, підготовка до лабораторного заняття з питань: 1. Забезпечення цілісності і достовірності інформації 2. ДСТУ 7564:2014 - український національний стандарт криптографічного захисту інформації (функція хешування «Купина»)	6	2
Знати: криптографічні механізми захисту криптовалюти	**Лекція 9. План лекції** 1. Криптовалюта. Криптоджекінг 2. Блокчейн технологія 3. Криптографічні засоби захисту криптовалюти **Список рекомендованих джерел:** Основний: 1,2,3 Додатковий: 9	2	
Вміти: створювати захист інформації за допомогою програмних засобів; використовувати системні ресурси для	**Самостійна робота студентів** Вивчення та доповнення матеріалу лекції, підготовка до лабораторного заняття	6	2

1	2	3	4
захисту інформації			
Вміти: створювати захист інформації за допомогою програмних засобів; використовувати системні ресурси для захисту інформації	**Лабораторна робота № 4**. *Створення алгоритму та програми криптографічного захисту* **Завдання на лабораторну роботу:** 1. Ознайомитися з методом шифрування за варіантом. 2. Розробити блок-схему алгоритму шифрування та розшифровування 3. Реалізувати формальні моделі у вигляді двох підсистем і модуля з мінімальним інтерфейсом 5. Зашифрувати наданий викладачем текст 6. Відправити програму шифрування, ключі і шифрограму викладачу і отримати шифровані результати перевірки роботи програми 7. Здійснити частотний аналіз отриманого шифротексту 8. Описати особливості реалізації завдання та варіанти застосування розробленого модуля 9. Підготувати звіт про виконання лабораторної роботи	4	8
Знати: стеганографічні методи захисту інформації	**Тема 3.** Комп'ютерна стеганографія **Лекція 10. План лекції** 1. Термінологія та сфери використання стеганографії 2. Стеганографічні методи захисту інформації 3. Протоколи стеганографічних систем **Список рекомендованих джерел:** Основний: 3,4,5 Додатковий: 9,10	2	
Вміти: захищати інформаційні системи за допомогою програмних засобів	**Самостійна робота студентів** Вивчення та доповнення матеріалу лекції, підготовка до лабораторного заняття з питань: 1. Цифрові водяні знаки 2. Методи вкладення інформації у комп'ютерні файли 3. Методи приховування інформації в зображеннях 4. Методи приховування інформації в аудіосигналах.	8	2
Вміти: захищати інформаційні	**Лабораторна робота 5** *Стеганографічний захист інформації* **Завдання на лабораторну роботу:**	4	8

1	2	3	4
системи за допомогою програмних засобів	1. Встановити та підготувати віртуальну машину з ОС Windows для виконання лабораторної роботи 2. Проаналізувати приклади програм стеганографічного захисту і встановити вибрані для виконання лабораторної роботи 3. Виконати процедури приховування та розкриття текстової інформації з медіа-файлами різних форматів 4. Розробити блок-схему алгоритму стеганографічного захисту інформації в файлах зображень 5. Реалізувати формальні моделі у вигляді двох підсистем і модуля з мінімальним інтерфейсом 6. Приховати наданий викладачем текст 7. Підготувати звіт про виконання лабораторної роботи		
Знати: склад, технологію застосування і алгоритми електронного цифрового підпису.	**Тема 4.** Склад, технологія застосування і алгоритми електронного цифрового підпису **Лекція 11. План лекції** 1. Підпис документів: призначення і властивості 2. Автентифікація документів і особливості шифрування ЕЦП 3. Склад цифрового підпису і технологія застосування ЕЦП **Список рекомендованих джерел:** Основний: 2,4,5,6 Додатковий: 9,12	2	
Знати: склад, технологію застосування і алгоритми електронного цифрового підпису.	**Самостійна робота студентів** Вивчення та доповнення матеріалу лекції, підготовка до лабораторного заняття з питань: 1. Дайджест документа 2. Алгоритм цифрового підпису DSA	4	2
Знати: склад, технологію застосування і алгоритми електронного цифрового підпису.	**Лекція 12. План лекції** 1. Схеми використання ЕЦП. Сертифікат ключа 2. Системи сертифікації відкритих ключів 3. Алгоритм цифрового підпису ECDSA **Список рекомендованих джерел:** Основний: 2,5,7 Додатковий: 12	2	
Знати: склад, технологію застосування і	**Самостійна робота студентів** Вивчення та доповнення матеріалу лекції, підготовка до лабораторного заняття з питань:	12	4

1	2	3	4
алгоритми електронного цифрового підпису.	1. Цифрові сертифікати в ОС Windows 2. Правила застосування і зберігання ЕЦП		
Знати: логічну структуру та компоненти PKI	**Лекція 13. План лекції** 1. Інфраструктура відкритих ключів (PKI) 2. Принципи генерації, розподілу та збереження ключів 3. Обмін ключами по алгоритму Діффі-Хеллмана. **Список рекомендованих джерел:** Основний: 2,5,6 Додатковий: 8,10	2	
Вміти: розробляти індивідуальні системи управління доступом і захистом комп'ютерних систем	**Самостійна робота студентів** Вивчення та доповнення матеріалу лекції, підготовка до лабораторного заняття з питань: 1. Принципи функціонування PKI 2. Логічна структура та компоненти PKI 3. Закон України «Про електронний цифровий підпис» 4. Алгоритм ЕЦП ДСТУ 4145	12	4
Вміти: розробляти індивідуальні системи управління доступом і захистом комп'ютерних систем	**Лабораторна робота 6** *Програма PGP для криптографічного захисту та підпису електронних документів* **Завдання на лабораторну роботу:** 1. Встановити та підготувати віртуальну машину з ОС Windows для виконання лабораторної роботи 2. Встановити програму PGP на віртуальну машину та ознайомитися з її інтерфейсом користувача 3. Засобами програми сформувати ключі для криптографічних перетворень інформації та для виконання електронного підпису 4. Передати викладачу ключову інформацію 5. Підготувати звіт про виконання лабораторної роботи 6. Зашифрувати звіт відкритим ключем викладача, підписати його своїм приватним ключем і відправити звіт викладачу для перевірки 7. Налаштувати систему захищеного електронного листування	4	8
Знати: принципи побудови і використання	**Тема 5.** Криптографічний інтерфейс додатків операційної системи WINDOWS (CRYPTOAPI) **Лекція 14. План лекції**	2	

1	2	3	4
функцій CryptoAPI	1. Кріптопровайдери в системі Windows. Принципи побудови і використання CRYPTOAPI 2. Використання функцій CRYPTOAPI для шифрування і розшифрування даних 3. Використання функцій CRYPTOAPI для отримання і перевірки електронного цифрового підпису. **Список рекомендованих джерел:** Основний: 5,6 Додатковий: 8,9		
Вміти: користуватися бібліотеками прикладних програм комп'ютерних систем по захисту інформації	**Самостійна робота студентів** Вивчення та доповнення матеріалу лекції, підготовка до лабораторного заняття з питань: 1. Створення і передача криптографічних ключів за допомогою функцій CRYPTOAPI.	8	6
Вміти: користуватися бібліотеками прикладних програм комп'ютерних систем по захисту інформації	**Лабораторна робота 7** *Використання функцій CRYPTOAPI для криптографічного захисту ПЗ* **Завдання на лабораторну роботу:** 1. Встановити та підготувати віртуальну машину з ОС Windows для виконання лабораторної роботи 2. Розробити програмне забезпечення з використанням бібліотек Microsoft CryptoAPI (за варіантом) 3. Дослідити працездатність створеного ПЗ 4. Підготувати звіт про виконання лабораторної роботи 5. Підготувати презентацію розробленого програмного продукту	4	8
Разом за семестр		***180***	***100***

6. 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. Навчальний посібник Чернівці.- Видавничий дом «Родовід», 2017. – 471с.
3. Кавун С.В. Інформаційна безпека. Навчальний посібник Харків: ХНЕУ, 2016. -213с.

4. Гончарова Л.Л. Основи захисту інформації в телекомунікаційних та комп'ютерних мережах. / Л.Л. Гончарова, А.Д. Возненко, О.І. Стасюк, Ю.О. Коваль – К., 2015. – 435 с., іл.160.
5. *Зубок М. І. Інформаційна безпека : Навчальний посібник для студентів вищих навч.закладів / М. І. Зубок. – К. : КНТЕУ, 2009. – 132с.*
6. *КавунС. В. Інформаційна безпека підручник / С. В. Кавун. – Харків : ХНЕУ, 2016. – 368с.*
7. 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, 2015. – 632с.

Додатковий

8. Концепція (основи державної політики) національної безпеки України від 21 грудня 2000 року №2171-111.
9. 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.
10. Положення про порядок здійснення криптографічного захисту інформації в Україні від 22 травня 1998 року № 505/98.
11. *Кормич Б. А. Інформаційна безпека:організаційно-правові основи: навч. посібник для студентів вузів / Б. А. Кормич. – К. : Кондор, 2015. – 384с.*
12. *Пашкова А. Т. Інформаційна безпека як складова національної безпеки А. Т. Пашкова // Безпека життєдіяльності. – Київ, 2014. – № 11. – С. 34-36.*
13. *Полянська В. Кібернетична безпека України в умовах розвитку глобальної інформаційної системи / В. Полянська // Підприємництво, господарство і право. – Київ, 2013. – № 7 (211). – С. 48-50.*

Internet-ресурси

14. Защита информации – режим доступу: *http://www.bseu.by/it/tohod/lekcii9_2.htm*
15. Захист інформації – режим доступу:

http://www.warning.dp.ua/tel28.htm
16. Безпека на прикладному рівні – режим доступу:

http://www.dut.edu.ua

7. **Контроль та оцінювання результатів навчання:** положення про оцінювання результатів навчання студентів і аспірантів наказ КНТЕУ №2891 від 16.09.2019р.

Під час вивчення дисципліни «Методи і засоби захисту інформації» 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).

8.4. **За порушення академічної доброчесності** студенти будуть притягнені до такої академічної відповідальності:

- повторне проходження оцінювання (контрольна робота, іспит, залік тощо);
- повторне проходження навчального курсу.