МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ
КАРПАТСЬКИЙ НАЦІОНАЛЬНИЙ УНІВЕРСИТЕТ
ІМЕНІ ВАСИЛЯ СТЕФАНИКА

Факультет/інститут **фізико-технічний**

Кафедра **комп'ютерної інженерії і електроніки**

СИЛАБУС НАВЧАЛЬНОЇ ДИСЦИПЛІНИ

Захист інформації

Освітня програма **Всі крім ОП галузей Е Природничі науки, математика та статистика, F Інформаційні технології**

Спеціалізація (за наявності) _____

Спеціальність **Всі крім спеціальностей галузей Е Природничі науки, математика та статистика, F Інформаційні технології**

Галузь знань **Всі крім галузей Е Природничі науки, математика та статистика, F Інформаційні технології**

Затверджено на засіданні кафедри
Протокол № __ від "_" ___ 202_ р.

м. Івано-Франківськ – 202_ р.

Зміст

1. Загальна інформація.....3
2. Опис дисципліни.....3
3. Структура курсу 5
4. Система оцінювання курсу.....8
5. Оцінювання відповідно до графіку навчального процесу 8
6. Ресурсне забезпечення 8
7. Контактна інформація.....9
8. Політика навчальної дисципліни.....10

1. Загальна інформація

Назва дисципліни	Захист інформації
Освітня(і) програма(и)	Всі крім ОП галузей Е Природничі науки, математика та статистика, F Інформаційні технології
Спеціалізація (за наявності)	
Спеціальність	Всі крім спеціальностей галузей Е Природничі науки, математика та статистика, F Інформаційні технології
Галузь знань	Всі крім галузей Е Природничі науки, математика та статистика, F Інформаційні технології
Освітній рівень	бакалавр
Статус дисципліни	Вибіркова
Курс / семестр	2 курс, 3 семестр
Розподіл за видами занять та годинами навчання (якщо передбачені інші види, додати)	3 кредити Лекції – 14 год. Практичні заняття – 16 год. Самостійна робота – 60 год.
Мова викладання	Українська
Посилання на сайт дистанційного навчання	https://d-learn.pnu.edu.ua

2. Опис дисципліни

Мета та цілі курсу:	Надати студентам другого курсу системні знання про загрози інформації та методи її захисту, сформувати практичні навички безпечної роботи з інформацією в освітньому й професійному середовищі з урахуванням правових та організаційних вимог.
Передумови	Базова комп’ютерна грамотність
Компетентності:	**Загальні компетентності (ЗК)** **ЗК1.** Здатність до абстрактного мислення, аналізу та синтезу. **ЗК2.** Здатність застосовувати знання у практичних ситуаціях. **ЗК3.** Здатність до пошуку, аналізу та критичної оцінки інформації з різних джерел. **ЗК4.** Здатність використовувати інформаційно-комунікаційні технології. **ЗК5.** Здатність діяти на основі етичних міркувань (принципів академічної доброчесності). **ЗК6.** Здатність усвідомлювати права та обов’язки як члена суспільства, дотримуватися правових норм. **ЗК7.** Здатність до міжособистісної взаємодії та роботи в команді. **ЗК8.** Здатність до відповідальної та безпечної діяльності в цифровому середовищі.

	Фахові компетентності (ФК) *(універсальні для гуманітарних спеціальностей)* **ФК1.** Здатність ідентифікувати загрози інформації в освітньому, професійному та суспільному середовищі. **ФК2.** Здатність застосовувати правові та організаційні механізми захисту інформації відповідно до чинного законодавства України. **ФК3.** Здатність забезпечувати конфіденційність персональних даних у професійній діяльності. **ФК4.** Здатність дотримуватися вимог інформаційної безпеки під час роботи з цифровими ресурсами та сервісами. **ФК5.** Здатність розпізнавати та протидіяти соціальній інженерії, маніпуляціям та інформаційним атакам. **ФК6.** Здатність формувати та підтримувати культуру інформаційної безпеки в колективі.
Програмні результати навчання:	**Програмні результати навчання (ПРН)** Після завершення вивчення дисципліни студент повинен: **ПРН1.** Пояснювати основні поняття та принципи захисту інформації. **ПРН2.** Аналізувати загрози інформаційній безпеці та оцінювати можливі ризики. **ПРН3.** Орієнтуватися в нормативно-правових актах України щодо захисту інформації та персональних даних. **ПРН4.** Застосовувати організаційні та базові технічні засоби захисту інформації. **ПРН5.** Виявляти ознаки соціальної інженерії та фішингових атак. **ПРН6.** Дотримуватися принципів цифрової гігієни та безпечної поведінки в мережі Інтернет. **ПРН7.** Забезпечувати дотримання академічної доброчесності та етичних норм під час роботи з інформацією. **ПРН8.** Аргументовано обґрунтовувати вибір заходів захисту інформації в типових професійних ситуаціях.

2.1. Відповідність «Компетентності → ПРН»

Компетентності	ПРН
ЗК1, ЗК2, ЗК3	ПРН1, ПРН2
ЗК4, ЗК8	ПРН4, ПРН6
ЗК5, ЗК6	ПРН3, ПРН7
ЗК7	ПРН8
ФК1–ФК3	ПРН2, ПРН3
ФК4–ФК6	ПРН4–ПРН8

2.2. Відповідність ПРН ↔ методи навчання ↔ оцінювання

ПРН	Зміст ПРН	Методи навчання	Форми та методи оцінювання
ПРН1	Пояснює базові поняття та принципи захисту інформації	лекції з презентаціями, проблемне пояснення	тестові завдання, усне опитування
ПРН2	Аналізує загрози та оцінює ризики	кейс-метод, робота в малих групах	аналіз кейсу, письмове завдання

ПРН3	Орієнтується в законодавстві з ІБ	лекція, робота з нормативними актами	тест + аналітичні запитання
ПРН4	Застосовує організаційні та базові технічні заходи	практичні заняття, демонстрації	практична робота, чеклист
ПРН5	Виявляє соціальну інженерію та фішинг	аналіз прикладів, рольові вправи	практичне завдання
ПРН6	Дотримується цифрової гігієни	практичні заняття, самодіагностика	аудит цифрової безпеки
ПРН7	Дотримується академічної доброчесності	дискусія, аналіз ситуацій	ситуаційні завдання
ПРН8	Обґрунтовує вибір заходів захисту	міні-проєкт, презентація	захист міні-проєкту

3. Структура курсу

3.1. Структура курсу та розподіл годин

№	Тема	Лекції	Практичні	Самостійна робота	Разом
1	Основи захисту інформації	2	2	8	12
2	Загрози, ризики та порушники	2	2	8	12
3	Правові та етичні основи захисту інформації	2	2	8	12
4	Організаційні методи захисту інформації	2	2	8	12
5	Технічні засоби захисту інформації	2	4	12	18
6	Соціальна інженерія та людський фактор	2	2	8	12
7	Безпека в інтернеті та мобільних середовищах	2	2	8	12
	Разом	**14**	**16**	**60**	**90**

3.2. Зміст курсу

№	Тема	Результати навчання	Завдання
1.	Тема 1. Основи захисту інформації • Поняття інформації та ІБ • Інформація як ресурс • Тріада CIA • Класифікація інформації • Приклади інцидентів	Після опанування теми здобувач вищої освіти **повинен бути здатним**: 1. **Пояснювати** сутність інформації як об’єкта захисту та її роль у сучасному суспільстві. 2. **Визначати** поняття інформаційної безпеки та її основні складові. 3. **Характеризувати** принципи конфіденційності, цілісності та доступності (тріада CIA). 4. **Класифікувати**	аналіз реального інциденту

№	Тема	Результати навчання	Завдання
		інформацію за рівнем доступу та цінності. 5. **Наводити приклади** типових порушень інформаційної безпеки у навчальному, професійному та повсякденному середовищі. 6. **Пояснювати** наслідки порушення інформаційної безпеки для особи, організації та суспільства.	
	Тема 2. Загрози, ризики та моделі порушника • Класифікація загроз • Внутрішній і зовнішній порушник • Поняття ризику • Основи управління ризиками	Після опанування теми здобувач вищої освіти **повинен бути здатним**: 1. **Розрізняти** основні типи загроз інформаційній безпеці (технічні, організаційні, соціальні). 2. **Класифікувати** загрози за джерелом походження (внутрішні та зовнішні). 3. **Пояснювати** поняття інформаційного ризику та його складові. 4. **Аналізувати** типові сценарії порушення інформаційної безпеки. 5. **Описувати** модель порушника, його можливості та мотивацію. 6. **Оцінювати** можливі наслідки реалізації загроз для особи, організації або спільноти. 7. **Аргументувати** необхідність впровадження заходів захисту на основі оцінки ризиків.	побудова простої моделі загроз
	Тема 3. Правові та етичні основи захисту інформації • Законодавство України • Персональні дані • Комерційна та службова таємниця • Авторське право	Після опанування теми здобувач вищої освіти **повинен бути здатним**: 1. **Пояснювати** роль правового регулювання у сфері захисту інформації. 2. **Орієнтуватися** в	аналіз нормативного документа

№	Тема	Результати навчання	Завдання
	• Академічна доброчесність	основних нормативно-правових актах України щодо захисту інформації та персональних даних. 3. **Розрізняти** правові режими інформації (персональні дані, службова інформація, комерційна таємниця, публічна інформація). 4. **Пояснювати** права та обов'язки суб'єктів інформаційних відносин. 5. **Аналізувати** типові порушення законодавства у сфері захисту інформації та їх наслідки. 6. **Дотримуватися** принципів академічної доброчесності під час роботи з інформацією. 7. **Оцінювати** етичні аспекти використання інформації в навчальній і професійній діяльності.	
	Тема 4. Організаційні методи захисту інформації • Політика ІБ • Розмежування доступу • Управління інцидентами • Навчання користувачів	Після опанування теми здобувач вищої освіти **повинен бути здатним**: 1. **Пояснювати** роль організаційних заходів у системі захисту інформації. 2. **Характеризувати** основні елементи політики інформаційної безпеки організації. 3. **Розрізняти** рівні доступу до інформації та відповідальність користувачів. 4. **Пояснювати** принципи розмежування доступу до інформаційних ресурсів. 5. **Описувати** порядок дій у разі виникнення інцидентів інформаційної безпеки. 6. **Аналізувати** роль людського фактора в	розробка фрагмента політики ІБ

№	Тема	Результати навчання	Завдання
		забезпеченні інформаційної безпеки. 7. **Обґрунтовувати** необхідність навчання персоналу та формування культури інформаційної безпеки.	
	Тема 5. Технічні засоби захисту інформації • Захист комп'ютерних систем • Антивірусні засоби • Оновлення ПЗ • Мережевий захист • Основи криптографії • Резервне копіювання	Після опанування теми здобувач вищої освіти **повинен бути здатним**: 1. **Пояснювати** призначення технічних засобів у системі захисту інформації. 2. **Розрізняти** основні види технічних засобів захисту (захист комп'ютерів, мереж, даних). 3. **Пояснювати** принципи роботи антивірусних засобів та оновлення програмного забезпечення. 4. **Описувати** базові механізми захисту інформації в мережах (паролі, брандмауери, VPN — на концептуальному рівні). 5. **Пояснювати** призначення та принципи шифрування інформації без заглиблення в математичні алгоритми. 6. **Пояснювати** роль резервного копіювання у забезпеченні доступності та цілісності інформації. 7. **Застосовувати** базові технічні заходи захисту інформації у власній навчальній діяльності (2FA, безпечні налаштування).	шифрування файлів; налаштування 2FA; аналіз антивірусного захисту
	Тема 6. Соціальна інженерія та людський фактор • Соціальна інженерія • Фішинг, смішинг, вішинг	Після опанування теми здобувач вищої освіти **повинен бути здатним**: 1. **Пояснювати** сутність соціальної інженерії як	виявлення фішингових повідомлень

№	Тема	Результати навчання	Завдання
	• Психологічні методи впливу	одного з основних джерел загроз інформаційній безпеці. 2. **Розрізняти** основні види соціальної інженерії (фішинг, смішинг, вішинг, підміна довіри). 3. **Пояснювати** психологічні механізми впливу, що використовуються зловмисниками. 4. **Виявляти** ознаки соціальної інженерії та інформаційних маніпуляцій у типових ситуаціях. 5. **Аналізувати** приклади соціотехнічних атак у навчальному, професійному та побутовому середовищі. 6. **Застосовувати** правила безпечної поведінки для запобігання соціотехнічним атакам. 7. **Формувати** відповідальне ставлення до власної інформаційної поведінки та поведінки колективу.	
	Тема 7. Безпека в інтернеті та мобільних середовищах • Парольна політика • Хмарні сервіси • Соціальні мережі • Мобільні пристрої	Після опанування теми здобувач вищої освіти **повинен бути здатним**: 1. **Пояснювати** основні принципи цифрової безпеки користувача в сучасному інформаційному середовищі. 2. **Застосовувати** правила створення та управління надійними паролями. 3. **Використовувати** двофакторну автентифікацію для захисту облікових записів. 4. **Оцінювати** ризики, пов’язані з використанням	аудит власної цифрової безпеки

№	Тема	Результати навчання	Завдання
		соціальних мереж та хмарних сервісів. 5. **Дотримуватися** правил безпечної роботи з мобільними пристроями та публічними мережами. 6. **Аналізувати** власну цифрову поведінку з точки зору інформаційної безпеки. 7. **Формувати** індивідуальні рекомендації щодо підвищення рівня особистої цифрової безпеки.	

4. Система оцінювання курсу

Накопичування балів під час вивчення дисципліни	
Види навчальної роботи	Максимальна кількість балів
Лекції	20
Практичні заняття	60
Самостійна робота	20
Індивідуальне завдання	-
Максимальна кількість балів	100

4.1. Тестовий контроль за лекційним матеріалом

(два тестування протягом курсу)

Загальна характеристика тестів

- Кількість тестів: 2
- Кількість запитань у кожному тесті: 40
- Тип контролю: поточний контроль знань
- Форма проведення: d-learn
- Час виконання: 40–50 хвилин
- Кількість спроб: 1
- Допоміжні матеріали: не дозволяються

Тематичне наповнення тестів

Тест 1 (після Тем 1–3)

- Основи захисту інформації
- Загрози, ризики, модель порушника
- Правові та етичні основи ІБ

Тест 2 (після Тем 4–7)

- Організаційні методи захисту
- Технічні засоби (базовий рівень)
- Соціальна інженерія
- Цифрова безпека користувача

Типи тестових завдань

- вибір однієї правильної відповіді;
- вибір кількох правильних відповідей;

Критерії оцінювання тесту
(100-бальна шкала)
Оцінювання одного тесту

- Кількість запитань: 40
- Вага одного правильного запитання: 2,5 бала
- Максимум за тест: 100 балів

Пороговий рівень

- Мінімальний прохідний бал: 50
- Мінімальна кількість правильних відповідей: 20 із 40

4.2. На самостійну роботу виноситься розробка міні-проєкту на теми (на вибір):
Загальні вимоги до міні-проєкту

- форма виконання: письмовий звіт + презентація;
- обсяг: 5–8 сторінок + 10–12 слайдів;
- форма захисту: письмове обґрунтування;
- виконання: індивідуально або в парах.

---

1. Інформаційна безпека в освітньому середовищі

1. Аналіз загроз інформаційній безпеці університету.
2. Захист персональних даних студентів і викладачів.
3. Інформаційна безпека систем дистанційного навчання.
4. Політика інформаційної безпеки закладу вищої освіти (фрагмент).
5. Роль студентів у забезпеченні інформаційної безпеки університету.

---

2. Персональні дані та правовий захист інформації

6. Захист персональних даних у соціальних мережах.
7. Аналіз типових порушень законодавства щодо персональних даних.
8. Права та обов’язки користувачів у цифровому середовищі.
9. Інформаційна безпека та академічна доброчесність.
10. Етичні аспекти використання цифрової інформації.

---

3. Соціальна інженерія та інформаційні маніпуляції

11. Аналіз фішингових атак (реальні приклади).
12. Соціальна інженерія як загроза для організацій.
13. Психологічні методи впливу в інформаційних атаках.
14. Маніпуляції в соціальних мережах та їх наслідки.
15. Інформаційна безпека та дезінформація.

---

4. Цифрова безпека користувача

16. Аналіз власної цифрової безпеки (самоаудит).
17. Безпечне використання мобільних пристроїв.
18. Управління паролями та автентифікація користувачів.
19. Ризики використання публічних Wi-Fi мереж.
20. Хмарні сервіси: переваги та загрози.

---

5. Організаційні та управлінські аспекти ІБ

21. Організаційні методи захисту інформації в установі.
22. Людський фактор у системі інформаційної безпеки.
23. Навчання персоналу як елемент захисту інформації.
24. Реагування на інциденти інформаційної безпеки.

25. Формування культури інформаційної безпеки в колективі.

---

6. Міждисциплінарні та прикладні теми

26. Інформаційна безпека в діяльності державних органів.
27. Захист інформації у громадських та волонтерських організаціях.
28. Інформаційна безпека малого бізнесу.
29. Цифрова безпека журналістської діяльності.
30. Інформаційна безпека у сфері культури та медіа.

---

7. Аналітичні та рефлексивні міні-проєкти

31. Аналіз відомого інциденту витоку даних.
32. Наслідки порушення інформаційної безпеки для суспільства.
33. Порівняння організаційних та технічних методів захисту.
34. Інформаційна безпека як елемент національної безпеки.
35. Майбутні виклики інформаційної безпеки.

4.3. Критерії оцінювання практичних занять

Практичне заняття 1. Аналіз інцидентів інформаційної безпеки

Критерій	**Бали**
Коректне визначення суті інциденту	20
Виявлення порушених принципів ІБ (CIA)	20
Аналіз причин і наслідків	30
Обґрунтовані висновки та рекомендації	20
Оформлення/структурованість	10
Разом	**100**

Практичне заняття 2. Моделювання загроз, ризиків і порушника

Критерій	**Бали**
Ідентифікація загроз (не менше 5 релевантних)	25
Опис моделі порушника (тип, мотивація, можливості)	25
Якісна оцінка ризиків (ймовірність/вплив)	20
Запропоновані заходи реагування/пом’якшення	20
Чіткість і логічність подання	10
Разом	**100**

Практичне заняття 3. Аналіз нормативно-правових актів у сфері ІБ

Критерій	**Бали**
Правильний добір НПА під ситуацію	20
Виділення ключових норм/вимог	25
Аналіз відповідальності/наслідків порушення	25
Застосування норм до кейсу (висновок)	20
Оформлення та коректність термінів	10
Разом	**100**

Практичне заняття 4. Розробка фрагмента політики інформаційної безпеки

Критерій	**Бали**
Наявність обов’язкових елементів політики (ціль, сфера, ролі)	20
Правила доступу/роботи з даними сформульовані чітко	25
Узгодженість із загрозами та ризиками (логіка “загроза → правило”)	25
Реалістичність і практична застосовність	20
Якість оформлення	10
Разом	**100**

Практичне заняття 5. Технічні засоби захисту інформації
(антивірус/оновлення/налаштування безпеки ОС і браузера/мережеві основи/шифрування та резервне копіювання — на базовому рівні)

Критерій	**Бали**
Правильний вибір і пояснення технічних засобів (що і навіщо)	25
Коректність виконання дій/демонстрації (за інструкцією)	30
Дотримання безпечних налаштувань (оновлення, права доступу тощо)	20
Інтерпретація результатів (що змінилось, який ефект)	15
Оформлення звіту/скріншоти/структура	10
Разом	**100**

Практичне заняття 6. Базові практики користувача: паролі, 2FA, резервне копіювання

Критерій	**Бали**
Налаштовано/описано коректно (паролі/2FA/backup)	35
Пояснено призначення та ризики, які закриває кожен захід	25
Якість запропонованого “персонального набору правил”	20
Самооцінка ризиків і висновки	10
Оформлення результатів	10
Разом	**100**

Практичне заняття 7. Виявлення фішингу та соціотехнічних атак

Критерій	**Бали**
Виявлення ознак атаки (не менше 6 ознак)	30
Класифікація типу атаки (фішинг/смішинг/вішинг тощо)	20
Оцінка ризиків і потенційних наслідків	20
Запропоновані заходи протидії/поведінковий алгоритм	20
Логічність і чіткість відповіді	10
Разом	**100**

Практичне заняття 8. Аудит особистої цифрової безпеки

Критерій	**Бали**
Повнота аудиту (чеклист + приклади)	30
Виявлення ключових слабких місць	25
Реалістичний план покращення (мін. 5 кроків)	25
Усвідомленість і відповідальність висновків	10
Оформлення	10
Разом	**100**

4.4. Критерії оцінювання міні-проєкту

Критерій оцінювання	**Максимальна кількість балів**
Відповідність темі та програмним результатам навчання (ПРН)	30 балів
Логічність, аргументованість та повнота викладу матеріалу	30 балів
Використання нормативних, наукових та аналітичних джерел	20 балів
Оформлення роботи та якість презентації результатів	20 балів
Разом (ваговий коефіцієнт – 0,2)	**100 балів**

Деталізація

- **90–100 балів** — повне розкриття теми, чітке обґрунтування, коректне використання джерел, високий рівень оформлення.
- **75–89 балів** — тема розкрита достатньо, незначні неточності або логічні прогалини.
- **60–74 бали** — базовий рівень, поверхневий аналіз, обмежене використання джерел.
- **менше 60 балів** — фрагментарні знання, відсутність логіки або невідповідність темі.

5. Оцінювання відповідно до графіку навчального процесу

Види навчальної роботи	Навчальні тижні																	Разом
	1	2	3	4	5	6	7	8	КСР	9	10	11	12	13	14	15	КСР	
Лекції (ваг.коеф. 0,2)									100								100	20
Практичні заняття (ваг.коеф. 0,6)		100		100		100		100			100	100		100		100		60
Самостій-на робота (ваг.коеф. 0,2)																	100	20
Всього за тиждень		100		100		100		100	100		100	100		100		100	200	100

6. Ресурсне забезпечення

Матеріально-технічне забезпечення	мультимедійний проєктор, комп’ютерний клас, доступ до мережі Інтернет.

Література

1.1. Обов’язкова література

Нормативно-правові акти України

1. Конституція України.
2. Закон України «Про інформацію».
3. Закон України «Про захист інформації в інформаційно-комунікаційних системах».
4. Закон України «Про захист персональних даних».
5. Закон України «Про доступ до публічної інформації».
6. Закон України «Про основні засади забезпечення кібербезпеки України».

Навчальні видання

7. Баранов О.А. *Інформаційна безпека*. – К.: Наукова думка.
8. Ліпкан В.А. *Інформаційна безпека України*. – К.: КНТ.
9. Довгань О.Д. *Правове забезпечення інформаційної безпеки*. – К.: Юрінком Інтер.

1.2. Додаткова література та ресурси

10. ISO/IEC 27001 — Information Security Management Systems (огляд).
11. ISO/IEC 27002 — Code of practice for information security controls (огляд).
12. GDPR (EU) — загальні принципи захисту персональних даних.
13. Schneier B. *Secrets and Lies*.
14. Mitnick K. *The Art of Deception*.
15. Floridi L. *Information Ethics*.
16. Почепцов Г.Г. *Інформаційні війни*.

Онлайн-ресурси

17. CERT-UA — рекомендації та попередження.
18. Національний координаційний центр кібербезпеки України.
19. ENISA — аналітичні матеріали (оглядово).

Таблиця відповідності «Тема → джерела»

№ теми	Назва теми	Обов'язкова література	Додаткова література
1	Основи захисту інформації	1, 2, 7	10, 13
2	Загрози, ризики та моделі порушника	7, 8	13, 14
3	Правові та етичні основи захисту інформації	1–6, 9	12, 15
4	Організаційні методи захисту інформації	7, 8	10, 11
5	Технічні засоби захисту інформації	7	10, 11, 13
6	Соціальна інженерія та людський фактор	7, 8	14, 16
7	Цифрова безпека користувача	2, 4, 7	17–19

7. Контактна інформація

Кафедра	Комп'ютерної інженерії та електроніки, вул. Шевченка, 57, 210а, 59-60-07, https://kkite.cnu.edu.ua/, kkie@cnu.edu.ua
Викладач (і) Гостьові лектори	Запухляк Руслан Ігорович, к.ф.-м.н., доцент
Контактна інформація викладача	ruslan.zapukhlyak@cnu.edu.ua

8. Політика навчальної дисципліни

Академічна доброчесність	Студент повинен бути толерантним і поважати думку інших. Заперечення

	повинні формулюватися тільки в коректній формі. Плагіат та академічна недоброчесність несумісні з принципами діяльності ЗВО. Не допускається підказування та списування під час здачі будь-яких робіт поточного, рубіжного чи підсумкового контролю. Не допускається користування телефонами та будь-якими іншими електронними засобами під час здачі будь-яких робіт поточного, рубіжного, чи підсумкового контролю. Недотримання принципів академічної доброчесності, списування, плагіат, використання сторонніх електронних засобів під час контролю знань заборонені. За недотримання академічної доброчесності, студент може бути недопущений до складання підсумкового контролю та відрахований з університету.
Пропуски занять (відпрацювання)	-1 бал за кожне заняття, пропущені заняття відпрацьовуються у встановленому кафедрою порядку.
Виконання завдання пізніше встановленого терміну	-20% балів від отриманого результату
Невідповідна поведінка під час заняття	-50% балів від отриманого результату
Додаткові бали	Додається до 10 балів за вчасне виконання всіх видів контролю, відвідування всіх занять, належну поведінку. Якщо у підсумку кількість балів є більшою за 100 балів, то підсумкова оцінка встановлюється така, що дорівнює 100.
Неформальна освіта	Можливість зарахування. Рекомендовані платформи: Coursera, Prometheus.

Викладач  Р.І. Запухляк